Nos. 13-50572, 13-50578, 13-50580, 14-50051

IN THE UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff—Appellee,

v.

BASAALY SAEED MOALIN,
MOHAMED MOHAMED MOHAMUD,
ISSA DOREH, and
AHMED NASIR TAALIL MOHAMUD,

Defendants—Appellants.

Appeal from the United States District Court
for the Southern District of California
Honorable Jeffrey T. Miller, Senior District Judge, Presiding

APPELLANTS' JOINT OPENING BRIEF

Joshua L. Dratel
Joshua Dratel, P.C.
2 Wall street, 3rd Floor
New York, NY 10005
212-732-0707
Attorney for Moalin

(Additional Counsel on Next Page)

Jameel Jaffer
Alexander A. Abdo
Patrick Toomey
Brett Max Kaufman
American Civil Liberties Union
125 Broad Street, 18th Floor
New York, NY 10004
212-519-7814 (Jaffer)
212-549-2517 (Abdo)
212-519-7816 (Toomey)
212-549-2603 (Kaufman)
Attorneys for Moalin

David J. Zugman
Burcham & Zugman
1010 2nd Ave., Suite 1800
San Diego, California 92101
(619) 699-5931
Attorney for M. M. Mohamud

Elizabeth Armena Missakian
Law Office of Elizabeth A. Missakian
P.O. Box 601879
San Diego, CA 92160
619-233-6534
Attorney for Issa Doreh

Benjamin L. Coleman
Coleman & Balogh LLP
1350 Columbia Street, Suite 600
San Diego, California 92101
Telephone: (619) 794-0420
Attorney for Ahmed Nasir Taalil Mohamud

QUESTIONS PRESENTED FOR REVIEW

I. In seizing the telephony metadata of Moalin, did the government act beyond the authority granted to it by 50 U.S.C. §1861?

II. Did the government violate Appellants' First and Fourth Amendment rights by seizing the personal metadata of Moalin (and millions of other Americans) and using it to pursue this criminal case?

III. Were Appellants deprived of their right to access and present exculpatory evidence regarding the investigation of Moalin in the early 2000's that concluded he was not involved in terrorism?

IV. Did the district court properly exclude evidence that Moalin was opposed to al-Shabaab because the proffered evidence was from 2009 and the indictment charged 2007-08 acts? Did the district court properly deny Appellants' motion to allow the videotaped deposition of a witness with exculpatory evidence? Did the district court allow unduly prejudicial and irrelevant material in allowing the government to present evidence about the "Black Hawk Down" incident when it was factually unrelated to any of the charges?

V. Did sufficient evidence support Issa Doreh's convictions?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

FEDERAL STATUTES

FEDERAL RULES

OTHER AUTHORITIES

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BASAALY SAEED MOALIN, MOHAMED MOHAMED MOHAMUD, ISSA DOREH, and AHMED NASIR TAALIL MOHAMUD, Defendants-Appellant.	)	Court of Appeal Case No. 13-50572, 13-50578, 13-50580, 14-50051 U.S. District Court, Southern District of California Case No. 10cr4246JM

INTRODUCTION

This Brief on Appeal is submitted on behalf of Defendants-Appellants, Basaaly Moalin, Mohamed Mohamed Mohamud, Issa Doreh, and Ahmed Nasir Taalil Mohamud, and challenges their convictions after trial in the Southern District of California on charges of material support to terrorists, material support to a Foreign Terrorist Organization, and money laundering (and/or conspiracy to commit those offenses). This case involves the nation — more accurately, the failed state — of Somalia, and the armed conflict and humanitarian crisis that has been ongoing there, on the Horn of Africa, for 25 years unabated by international and Somali efforts to

establish a stable, effective national government that is accepted by Somalis and recognized by the international community. As discussed below, and explored in detail at trial, the Somali *diaspora*, a substantial portion of whom reside in the United States, maintains an overriding political, social, and emotional interest in a peaceful and enduring outcome to what has been a quarter century of crises and seemingly endless cycles of catastrophic drought and consequent devastating famine, internecine violence, foreign invasion, and an abject absence of the civic and coordinated infrastructure that we take very much for granted. Indeed, in 1992 Human Rights Watch described Somalia as the "the worst humanitarian disaster in the world." *See* http://www.hrw.org/reports/1992/somalia/.

The defendants are members of that Somali *diaspora*, and were prosecuted and convicted for transmitting funds back to Somalia; a routine practice for Somalis eager to provide economic assistance for their families and others who remain in Somalia. The Indictment alleges that the money at issue in this case ($15,900 total) was earmarked for al-Shabaab, an indigenous Somali organization designated by the United States in February 2008 – the midpoint of the time period covered by the Indictment – as a Foreign Terrorist Organization ("FTO"). *See* http://www.state.gov/j/ct/rls/other/des/102446.html.

Defendants, however, deny that was the purpose for which the funds were

intended. Rather, the funds, consistent with contributions by the San Diego Somali community for all the years it has existed in the U.S., were designed to provide a regional Somali administration with humanitarian assistance relating to drought relief, educational services, orphan care, and security.

STATEMENT OF JURISDICTION

A. Nature of the Case

1. District court jurisdiction

This appeal is from the convictions of Basaaly Moalin, Mohamed Mohamud, Issa Doreh, and Ahmed Nasir Taalil Mohamud in the United States District Court for the Southern District of California before the Honorable Jeffrey T. Miller. The district court had jurisdiction under 18 U.S.C. § 3231.

2. Ninth Circuit Jurisdiction

This Court has jurisdiction over appeals from final judgments under 28 U.S.C. § 1294(1).

3. Finality of Judgment

A judgment of conviction in a federal criminal case is a final order subject to appeal under 28 U.S.C. § 1291.

4. Timeliness of Appeals

Appellants timely appealed their judgments. The district court sentenced

Moalin, Mohamed Mohamud, and Doreh on November 18, 2013. (CR 389-391, 392-394 (written judgments); ER 87-98.)[1] Moalin, Mohamud, and Doreh filed their notices of appeal by November 29, 2013. (CR 395, 398, 401; ER103-108.) Ahmed Mohamud was sentenced on January 31, 2014. (CR 430-31; ER 99-102.) He filed his notice of appeal on February 7, 2014. (CR 451; ER 106.)

5. Bail Status

All appellants are in custody serving their sentences. Their release dates are:

- Basaaly Moalin: July 6, 2026
- Mohamed Mohamud: February 27, 2022
- Issa Doreh: July 20, 2019
- Ahmed Nasir: February 22, 2016

(http://www.bop.gov/inmateloc/ accessed October 16, 2015.)

B. Proceedings and Disposition in the Trial Court

Defendants were charged by a Second Superseding Indictment filed on June 8, 2012, which alleged the following:

> Count 1: Conspiracy to provide material support to terrorists, in violation of 18 U.S.C. § 956 [conspiracy to kill persons in a foreign country] and 2332a(b) [conspiracy to use a weapon of mass destruction outside of the United States], all in violation of § 2339A(a).

---

[1] "CR" refers to the Clerk's Record and "ER" refers to the Appellants' Excerpts of Record and will be followed by volume number.

Count 2: Conspiracy to provide material support to a foreign terrorist organization in violation of 18 U.S.C, § 2339B(g)(6), all in violation of 18 U.S.C. § 2339B(a)(1).

Count 3: Conspiracy to launder monetary instruments, with the intent to provide material support to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1), providing material support to terrorists in violation of 18 U.S.C. § 2339A(a); and conspiracy to kill persons in a foreign country, in violation of 18 U.S.C. § 956, all in violation of 18 U.S.C. § 956, all in violation of 18 U.S.C. § 1956(a)(2)(A) and (h).

Count 4: To Moalin only, conspiracy to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a) [Count Four) and providing material support to foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1) and 2 [Count Five].

Count 5: Providing material support to a foreign terrorist organization in violation of 18 U.S.C. 2339B(a)(1) and (2) on or about April 23, 2008.

(CR 147; ER1–12.)

Trial commenced on January 28, 2013 and on February 22, 2013, the jury returned guilty verdicts on all counts against all defendants. (CR 302.) After the now infamous Edward Snowden revelations, Appellants moved for a new trial; the district court heard the motion on November 13, 2013 and denied it by amended order

November 18, 2013. (CR 388; ER 70.)

On April 10, 2014, appeal numbers 13-50571, 13-50578, 13-505890, and 14-50051 were consolidated by this Court.

STATEMENT OF THE ISSUES

The first issue in this appeal is whether the district court erred in failing to suppress evidence that was derived from unlawful surveillance conducted under 50 U.S.C. §1861, also known as Section 215 of the PATRIOT Act. Since 2006, the government has relied on that provision to collect telephony metadata relating to millions of U.S. residents—to assemble a record of who they called, when they called them, and how long they spoke for. This vast surveillance program is unlawful, as the Second Circuit has held. *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (declaring the program to be "unprecedented," "unwarranted," and *ultra vires*). In this case, the government relied on information obtained from the NSA's unlawful telephony-metadata program to obtain Foreign Intelligence Surveillance Act ("FISA") orders authorizing extensive surveillance of defendant Moalin's communications, and the government's case against the defendants was based almost entirely on evidence that was obtained through that surveillance. The trial court's failure to suppress the unlawfully obtained evidence is reason in itself to vacate defendants' convictions.

The district court erred in holding that the government's collection of

defendant Moalin's telephony metadata was lawful. As the Second Circuit has explained, and as government reviews have also concluded, the government's telephony-metadata program is based on an indefensibly broad reading of Section 215 (see Section I below). Moreover, even if Section 215 permitted the surveillance, the Fourth Amendment would not. Thirty-year old cases that addressed targeted metadata collection for short periods of time cannot reasonably be read to authorize dragnet and indefinite surveillance of hundreds of millions of people. Even if Section 215 were unclear, the doctrine of constitutional avoidance would compel the conclusion that Section 215 did not authorize the surveillance at issue here (see Section II below).

The government's failure to disclose exculpatory information, pursuant to *Brady v. Maryland*, 373 U.S. 83 (1963), provides a third reason to vacate the convictions (*see* Section III, below). As part of pretrial discovery, the government produced a Federal Bureau of Investigation ("FBI") intelligence assessment that disputed any claim that Moalin's intent in raising funds to send to Somalia was directed toward al-Shabaab. Moalin made motions for additional disclosure, but the government refused to provide any of the records underlying the FBI's assessment. It was only *after* trial that the government revealed that it had investigated Moalin in 2003 and concluded that he was not connected to terrorism and that his actions were

based upon clan loyalty. This information was precisely what Appellants had attempted to argue to the jury, and it cast doubt on the centerpiece of the government's theory: that Moalin's telephone conversations intercepted pursuant to FISA were with a leading al-Shabaab military and were meant to support terrorism. Post-trial disclosures, in other words, dramatically undermined the government's theory of the case and equally dramatically reinforced Moalin's defense. The district court also erred by precluding Defendants from presenting exculpatory evidence—even while it permitted the government to introduce the irrelevant and highly prejudicial "Black Hawk Down" tragedy (*see* Argument IV below). Regarding preclusion, the district court prohibiting Appellants from presenting evidence of their ideological opposition to the terrorist organization al-Shabaab. Moalin – before he could know that there was indictment against him – had organized a peace/women's right conference. Al-Shabaab is a militant Islamist group and as such is opposed to women's rights and to peace. Moalin's acts in organizing a women's rights/peace conference got him put on an al-Shabaab hit list. The district court precluded this evidence because the conference occurred after the acts alleged in the indictment. This ruling was an abuse of discretion since the point of the evidence was to show that Moalin was not a supporter of al-Shabaab since he held views antithetical to them and it made much less likely that he would have ever supported al-Shabaab in the first

place. In a similar vein, the district court abused its discretion in refusing to order a deposition, pursuant to Rule 15, Fed.R.Crim.P., of a crucial defense witness named in the Indictment as a recipient of some of the transferred funds at issue and he would disavow any connection to al-Shabaab.

While precluding exculpatory evidence, the district court overruled the Defense's Federal Rule of Evidence 403 objection to the government's presentation of the "Black Hawk Down" incident from 1993. "Black Hawk Down" is about how 18 American soldiers were massacred by a Somali mob in Mogadishu. It bore no relevance to the charges in the indictment, but it did point out an "us versus them" narrative about a heroic America getting slaughtered by enemies in Somalia. While lacking any relation to the charges of whether Appellants were financially supporting al-Shabaab, it did carry the implied finger-point that Appellants were aligned with people who were enemies of the United States. These evidentiary errors merit reversal both individually or collectively under a cumulative error analysis.

The final argument is Appellant Doreh's challenge to the sufficiency of the evidence against him with respect to all counts of conviction because the government failed to prove his knowledge that funds were destined for an FTO and/or terrorist activity, or that he intended any funds to be transmitted for that purpose.

STATEMENT OF THE FACTS

Defendants-Appellants Basaaly Moalin, Mohamed Mohamed Mohamud ("M. Mohamud"), and Issa Doreh, were indicted October 20, 2010 (CR 1), in a five-count Indictment unsealed November 2, 2010. All three defendants were remanded without bail (CR 16.) A Superseding Indictment added Ahmed Nasir Taalil Mohamud ("Nasir Mohamud") as a defendant. (CR 38.)

A. The Second Superseding Indictment

All five counts in the Second Superseding Indictment related to defendants' alleged transmission of money – a total of $15,900 (CR 147; ER 1-12) – from the U.S. to Somalia, purportedly in support of al-Shabaab, a Somali organization that was designated an Foreign Terrorist Organization by the U.S. Department of State February 26, 2008. (6RT[2] 1043.) The defense was that Appellants did not intend to send funds to support al-Shabaab, but rather to assist regional clan-based governmental administrations that existed in the absence of a unified, effective, central Somali government. *See United States v. Moalin*, 2013 U.S. Dist. LEXIS 164038 (S.D. Cal. Nov. 18. 2013).

Because the conduct at issue straddled that date of al-Shabaab's designation,

---

2 "RT" refers to the reporter's transcript of these proceedings with the leading number indicating which volume such that "6RT" refers to the sixth volume of the reporter's transcript.

only Counts Two and Five charged material support to a *designated* Foreign Terrorist Organization under §2339B. Counts One and Four charged material support as well, but under the generic terms of §2339A, which proscribes material support (or conspiracy to provide such support) to a conspiracy (in violation of 18 U.S.C. §956) to kill, maim, or kidnap overseas.

The Second Superseding Indictment alleged that over the course of just more than seven months – from January 1, 2008, through August 5, 2008 – the defendants transmitted a total of $15,900 to Somalia in twelve transactions conducted through a money exchange firm – a *hawala* – in San Diego, California. (CR 147.) The largest amount in any one transmission was $1,950. *Id*.[3]

Moalin, a naturalized U.S. citizen who emigrated to the U.S. from Somalia in 1996, and drove a taxi in San Diego, was alleged to have organized the transmittal of the funds and to have contributed his own money as well. M. Mohamud, an imam in

---

[3] Due to the lack of a central banking system in Somalia, it is necessary to utilize "*hawalas*" or private money transfer centers, to send money to Somalia. 440. The Somali community in San Diego used the Shidaal Express *hawala* to transfer money to Somalia. Moalin also used that same *hawala*. Sometime in 2009, a fraud investigation was commenced against Shidaal Express's owner. *S.E.C. v. Shidaal Express, Inc., and Mohamud Abdi Ahmed*, 09cv2610-JM (CASD); *United States v. Ahmed*, 10cr3170-DMS (CASD). It appears, from the discovery, that the investigation of Moalin was resumed as a result of that fraud investigation. Subsequent to the fraud investigation, the Indictment against Moalin was issued October 22, 2010.

the Somali community in San Diego, allegedly agreed to raise funds in his mosque for Moalin to send to Somalia. Doreh was an employee at the *hawala*, Shidaal Express, in San Diego. Nasir Mohamud, a resident of Anaheim, California, also allegedly contributed funds to those sent to Somalia via Shidaal Express.

Moalin was subject to electronic surveillance conducted pursuant to FISA from December 2007 through part of August 2008. (CR 123, Gov. Resp. to Suppression.) The government's position was that a party to a number of those calls, a person calling himself "Sheikalow," was in fact Aden Ayrow, an al-Shabaab military commander operating in Somalia. During some of those calls, which also included rambling political and social discussions, "Sheikalow" solicited money from Moalin (and M. Mohamud); the government alleged that the transferred funds to Somalia through the *hawala* were destined for Aden Ayrow and al-Shabaab.

B. Background of Appellants' Conduct and the Allegations in the Superseding Indictment

Somalia spans the northeast corner of Africa – the Horn of Africa – running South to Kenya, West to Ethiopia, Eritrea, and Djibouti, and bordered to the East by the Indian Ocean. *See* http://www.worldatlas.com/webimage/countrys/africa/so.htm.[4]

---

[4] Mercator projection makes the equatorial and boomerang shaped Somalia look smaller than it really is. Superimposed on the U.S., Somalia's northernmost and easternmost tip would be in New York State, its southernmost tip in Florida, and its westernmost tip in Indiana.

Controlled during the 19th and 20th centuries as the colonial property of the United Kingdom (the northern section of Somalia, sometimes known as Somaliland) and Italy (the central and southern sections, encompassing the capital city, Mogadishu, and nearly the entirety of the territory relevant not only to this case but to the crisis that has afflicted Somalia for the past 25 years).

The government called an expert witness to explain to this San Diego jury the recent history of Somalia so that the jury could understand the context of the government's charges. In presenting this testimony, the government tacitly concedes that adjudicating this case requires an understanding of the recent history of Somalia, including its enduring civil war, intermittent military incursions by Ethiopia, the lack of any effective central government, the underlying tribal, clan, and sub-clan allegiances that prevail among Somalis (including expatriates), the conditions of extreme deprivation, including famine, under which its population has suffered, and the general atmosphere of chaos and anarchy that pervades on a daily basis. Included within this history and background are the development and organization of the Union of Islamic Courts (hereinafter "UIC") and al-Shabaab – and later the Transitional Federal Government (hereinafter "TFG") – the timing and extent of Ethiopian military activity within Somalia, and the relevance, to the defendants, of Somalia's geography and their heritage.

The expert witness on Somalia was Matthew Bryden, a frequent government expert on Somalia.[5] He explained Somalia achieved independence in 1960, reconstituting itself as the Republic of Somalia. (3RT 449, 452.) A brief power vacuum created by the assassination of one of Somalia's early presidents was filled by a military coup, and in 1969 General Muhammad Siad Barre emerged as the new (military) president of Somalia. Although Barre set up the Somali Revolutionary Socialist Party, his government essentially remained a military dictatorship for 21 years. (3RT 453.) Under Barre, Somalia was initially a Soviet client state, but that relationship ended after Somalia attacked Ethiopia to annex lands inhabited by native Somalis; Moscow sided with the Ethiopians. (3RT 452.)

The Soviets' decision to support Ethiopia at Somalia's expense drove Gen. Barre in the opposite direction, and the United States became Somalia's patron state and provided up to $100 million in aid per year. *See* https://en.wikipedia.org/wiki/Siad_Barre. In conventional military dictator fashion, Gen. Barre's ruled through corruption and clan nepotism, which of course generated considerable opposition from those excluded from those benefits. *Id.*

Compounding those problems, Barre's human rights violations were among

---

5 Bryden also testified as an expert witness in *United States v. Ali*, 799 F.3d 1008 (8th Cir. 2015) and *United States v. Omar*, 786 F.3d 1104 (8th Cir.2015).

Africa's worst. *See, e.g., Yousuf v. Samantar*, 552 F.3d 371, 373-374 (4th Cir. 2009) ("[b]eginning in the late 1970s, opposition to the Barre regime developed within the disfavored clans and grew among the general citizenry following Somalia's unsuccessful war against Ethiopia over the Ogaden territory. The military leadership reacted by imposing harsh control measures against government opponents, including the alleged commission of 'numerous atrocities against ordinary citizens' in order to 'terrorize the civilian population and to deter it from supporting the growing opposition movements.' J.A. 33. Plaintiffs allege that government intelligence agencies, including the National Security Service ('NSS') and the military police, engaged in the widespread and systematic use of torture, arbitrary detention and extrajudicial killing against the civilian population of Somalia.' J.A. 33.").

As the cold-war ended and U.S. interest in funding anti-Soviet states declined, Barre lost the foreign aid basis for both his patronage and control of the army. As the wall fell in Germany, the state fell in Somalia. Rebellions in various parts of Somalia were common commencing in the late 1970's, and during the 1980's those rebel groups had multiplied and become more active. By 1989-90, in the midst of a protracted drought, the Barre government weakened sufficiently to permit rebel forces to migrate from central Somalia to Mogadishu. An uprising started in the capital at the end of December 1990.

The Barre government was eventually exiled soon thereafter. That abdication hurtled Somalia into a two-decade ongoing cycle of violent, devastating civil war. Deadly factional fighting, generally among competing Somali warlords armed with sophisticated weaponry, and divided along tribal, clan, and sub-clan lines, continued unabated for years, during which no central government existed. (3RT 428, 431.) The capital, Mogadishu, became a no-man's land.

Initially, Somalia was without a government in January 1991. However the rebel movement entered the capital and the United Somali Congress, composed of two factions, declared a transitional government. (3RT 343-455.) The two wings divided, though, and in November 1991 fighting began, creating a humanitarian crisis in Mogadishu as well as other parts of Somalia, and which led to the death of approximately 30,000 people in Mogadishu alone and the displacement of hundreds of thousands of others. (3RT 455.) This fighting, as well as drought conditions, led to famine conditions across much of southwest Somalia. (3RT 456.)

It should be noted that Somalia's civil war has *not* been a religious war of Islam displacing some other faith. Somalia is nearly completely Sunni Muslim. *Yousuf v. Samantar*, *supra,* 552 F.3d at 373-74. Islam remains today Somalia's official religion. *See* http://www.pewforum.org/files/2014/01/global-religion-full.pdf.

Instead, what has divided modern Somalia is not religion, but rather what has

always divided Somalia (as well as every other pre-industrial society ever investigated): clan rivalries. *See, generally*, Jared Diamond, *Guns, Germs and Steel* (W.W. Norton & Company: 1999). As the Seventh Circuit observed in 2006, "Somalia is a land of clans. . ." *Ahmed v. Gonzales*, 467 F.3d 669, 671 (7th Cir. 2006).[6]

In 1992, with the continuing humanitarian crisis (famine) aggravated by that civil war, the United States (and the United Nations) implemented Operation Restore Hope, which was designed to provide needed humanitarian aid to Somalia and police violent warlord activity. However, the infamous "Black Hawk Down" incident in October 1993 caused the U.S. and U.N. to withdraw their forces (and, for the U.S., *all* personnel) from Somalia by March 1994, leaving the populace again at the mercy of not only the varying warlords vying for hegemony, but also the Ethiopian army, which, capitalizing on the absence of any organized government in Somalia, periodically invaded Somalia as a means of promoting Ethiopia's perceived domestic and foreign policy objectives. From that point onward through the time encompassed

---

[6] *See also, e.g., Hussein v. AG of the United States,* 273 Fed. Appx. 147 (3d Cir. 2008) (unpublished), in addressing the torture claim, the Board reviewed the contents of the State Department's Bureau of Democracy, Human Rights, and Labor Report on Country Conditions for Somalia for 2005, and commented at length on the disturbing number of deaths since 1991 resulting from interfactional and interclan fighting, factional militia fighting for political power and control of territory, revenge reprisals, and other criminal activities").

by the Indictment, the U.S. did not have a formal, official presence, either militarily or diplomatically, in Somalia. (3RT 461.) The U.N. departed Somalia a year later. (*Id*.)

In 1995, two persons previously identified as warlords – General Mohamed Farah Aidid and Ali Mahdi – and each with different tribal allegiances, self-proclaimed themselves president of Somalia. That contest simply precipitated more systemic violence. In 1996, following General Aidid's death, Somalia was effectively balkanized until 2004, with various warlords controlling local territories.

Beginning in 2000, efforts were made to establish a stable, internationally recognized and assisted central government for Somalia. Somalia's Transitional Federal Government (hereinafter "TFG") was created in 2004. It initially consisted of a loose coalition of Somali leaders who ostensibly shared the goal of establishing a centralized national government. Abdullahi Yusuf Ahmed, a former military officer who had also previously been a warlord and had engaged in Somalia's factional fighting, was appointed as the TFG's first president.

However, during TFG's first two years of existence, President Yusuf remained in exile in Nairobi, and then in Baidoa (a city located in south central Somalia). Mogadishu was considered not only to be insecure , but in fact *hostile* to the new government (as were other broad sections of the Somali populace throughout the

country). (3RT 463.) President Yusuf immediately called for the deployment of 20,000 Ethiopian troops to protect him and to deliver his government back to Mogadishu. (3RT 464, 472.)

However, in the intervening period, while the TFG resided in the Baidoa area, in February 2006, local and tribal militia leaders formed a public partnership called the Alliance for the Restoration of Peace and Counterterrorism (hereinafter "ARPCT"), which was constituted to fight the groups attacking the TFG. However, because ARPCT was generally viewed as having the support of the CIA, it met opposition by the Somali public.

In response, according to a report written for the Council on Foreign Relations,

> [w]ith broad support from the public, clan leaders, Mogadishu's business community, and a preexisting network of *sharia* courts (known collectively as the Union of Islamic Courts, or UIC) banded together and, after a four-month battle in Mogadishu, handily defeated the ARPCT on June 5, 2006. The governing coalition that emerged from this victory named itself the Supreme Council of Islamic Courts (SCIC).

Bronwyn E. Bruton, *Somalia a New Approach*, Council on Foreign Relations, Council Special Report No. 52, March 2010.[7]

---

[7] The Council on Foreign Relations' web site describes Ms. Bruton as "a democracy and governance specialist with extensive experience in Africa[.]" Ms. Bruton has previously served as a program manager on the Africa team of the U.S. Agency for International Development's Office of Transition Initiatives. *See* http://www.cfr.org/experts/africa-democracy-promotion-ethiopia/bronwyn-e-bruton/b14483.

Thus, the UIC, an umbrella organization for courts in Mogadishu and other parts of southern Somalia, assumed control of Mogadishu. Although there had been Islamic courts practicing *sharia* (Islamic civil and religious) law in Somalia for some time, the number of such courts had increased from three or four in 1998 to more than 12 by 2006. (3RT 442.)

At that point, the UIC assumed responsibility for, and maintained, many of whatever governmental functions the central government had previously failed to provide in Somalia. The UIC also committed to combating corruption, internecine fighting, banditry, and clan-oriented predations. (3RT 476.) As described by another author, a Professor of Political Science at Valdosta State University in Georgia,

> the Islamic Courts' role in running Somalia met with mixed reaction. They were able to bring a likeness of law and order to a disorderly country by setting up schools and arbitrating internal disputes and dramatically reducing violence in areas under their control. A profile of the courts in 2006 showed eleven autonomous courts in Mogadishu alone whose roles included approving transactions such as buying houses and cars, overseeing weddings and divorces and expanding their authority across most of the capital while staying out of politics ("Somali's Islamic Courts," 2006). The factions that make up the Islamic Courts are distinguished by their interpretation of Islamic Sharia law, with the most conservative interpreting the law exactly to the letter. A militant group, al-Shabab, for example, which controls Southern Somalia, has been authoritarian and unaccountable, as opposed to Islamists who control the capital.

Napoleon A. Bamfo, "Ethiopia's Invasion of Somalia in 2006: Lessons Learned,"

African Journal of Political Science and International Relations, Vol. 4(2), pp. 055-065, February 2010 (hereinafter "Ethiopia's Invasion").[8]

Each Islamic Court also fielded a militia that functioned as a form of police force. Members wore a distinctive red head cloth and carried assault weapons and rocket-propelled grenades (hereinafter "RPG") launchers, and other light weapons. (3RT 477-478.) They drove pickup trucks or four-wheel-drive vehicles with the tops cut off and a heavy machine gun mounted on the back. (3RT 478.) RPG's were not limited to al-Shabaab; according to Bryden, anyone in Somalia who wanted an RPG (or other weaponry) could acquire one. (4RT 596.)

Hassan Dahir Aweys eventually emerged as a behind-the-scenes leader of the UIC, which was viewed, when it emerged in Mogadishu, as a direct challenge to the TFG. The UIC's expansion into territory across southern Somalia precipitated a direct confrontation with the TFG, and fighting ensued. In Summer 2006, the UIC gained control of Mogadishu. (3RT 484.) During the second half of 2006, peace talks between the TFG and the UIC broke down and clashes occurred outside Baidoa, threatening the TFG and Ethiopian forces stationed there. The Ethiopian offensive was rapid, and the UIC was defeated in central Somalia and in Mogadishu. (3RT 485.)

---

8 http://www.academicjournals.org/article/article1381826680_Bamfo.pdf

The TFG's installation in Mogadishu, sponsored by the Ethiopian military, did not resolve the crisis in Somalia. Many Somalis perceived the TFG as simply another puppet government beholden to Ethiopia, and infected with corruption and cronyism like the Barre regime. (3RT 453, 472.) Although not supported in its own country, the international community welcomed the TFG as Somalia's new interim government, and the U.N. accepted the TFG's representatives as Somalia's official representatives to the U.N. As a result, humanitarian aid began to flow anew to Somalia. (3RT 473.)

Conversely, the UIC went underground and emerged a few months later as part of a broad-based and complex insurgency against the Ethiopian intervention and the TFG, which the Ethiopian military had returned to Mogadishu by force. (3RT 486.) As Prof. Bamfo has explained, "[t]he Union of Islamic Courts (UIC) mobilized an opposition made up of clan militias and other insurgent groups that were united in their common goal of defeating the invading Ethiopian troops." *See* Ethiopia's Invasion, at 59. Although Ethiopia claimed that the initial invasion would be short in duration, its war against Somalia became protracted, and lasted until 2008.[9]

Somalia's indigenous defense against Ethiopia's invasion was waged primarily

---

[9] Ethiopia had previously invaded Somalia in 1996, with military engagements between Ethiopia's armed forces and Somali militias lasting until 2000. The two countries have had a history of armed conflict dating back to at least the 19th century. https://en.wikipedia.org/wiki/Ethiopian%E2%80%93Somali_conflict

by militias aligned with the UIC. However, those militias did not constitute an organized army under singular control of any particular entity. They were independent and autonomous, forming along geographic and tribal/clan/sub-clan lines. It was at that point that UIC's extremist, militant branch formed its own separate movement, emerging as al-Shabaab. (3RT 486.)

The U.S. designated al-Shabaab an FTO February 26, 2008. Notably, the U.S. did *not* designate (as an FTO) the UIC, or any of the other branches of that loosely affiliated umbrella organization.

Unfortunately, there is a synecdoche at work here. The term "al-Shabaab" is broad and it means "the youth." (4RT 514.) In this case, the government contended that whenever Appellants spoke of the "youth" they were referring to al-Shabaab and its incarnation as an FTO. Appellants' defense was that the government's view was overly simplistic, and that they were not necessarily referring to the same thing when they were talking about the "youth" or "al-Shabaab," the FTO. (4RT 635.)

The Ethiopian occupation of Somalia lasted three years, from 2006 to January 2009, when Ethiopian troops began withdrawing. (4RT 612.) As Bryden testified, in October 2007 he wrote in a confidential memo to the United States Agency for International Development (hereinafter "USAID") that "Ethiopian intervention in Somalia has triggered a persistent and escalating insurgency." (4RT 614-15.)

Also, according to Bryden at the time (and repeated during his cross-examination at trial), the U.S. was widely held responsible for Somalia's degeneration into a violent and costly occupation (by Ethiopian forces). Bryden had written (and acknowledged during cross-examination) that Ethiopia "accentuates the threat of terrorism in order to secure international, especially American, support." (4RT 614.).

As Bryden explained, in both Somalia and the Ethiopian/Somali regional state, Ethiopia had installed narrowly based compliant governments that lacked local legitimacy and disenfranchised segments of the population, thereby undermining U.S. interests, which Bryden described as regional stability and counterterrorism. However, as Bryden pointed out, utilizing the Ethiopians – in many respects, Somalia's historic enemy – to implement that policy had resulted in the reverse effect: creating radicalization and instability in Somalia. (4RT 616-17.)

Somalis bitterly resented and resisted the Ethiopian military presence as an occupying military force, and because it served to prop up the TFG. Also, Ethiopian troops were blamed for certain civilian deaths, destruction of property, and interference with local administration both directly through occupation and indirectly by supporting the TFG. The historic antagonism between Somalia and Ethiopia merely aggravated those problems. (4RT 614, 617.)

The scope of the problem for Somalis both in Somalia and in the diaspora was

massive. During the end of 2007 and into 2008, in addition to tens of thousands of Somali fatalities, Mogadishu remained uninhabitable for ordinary Somalis. The persistent violence, disease, and lack of civil services generated a massive displacement: hundreds of thousands of Somalis had fled the city and were instead living in ramshackle shanty towns by the sides of the main road exiting the city. Some are still there. (6RT 572, 644-47.)

Following the withdrawal of Ethiopian troops, President Yusef resigned. Sheik Sharif Ahmed, one of UIC's moderate leaders, was selected as TFG's president in January 31, 2009. According to Prof. Ken Menkhaus, that "selection signal[ed] a major power shift in the TFG toward the moderate Islamists within the former Islamic Courts Union." Ken Menkhaus, "Somalia After the Ethiopian Occupation,"[10] In addition, many other former members of the UIC are now involved with the TFG.

During the entire period of political strife, droughts and famine – including another severe episode in 2006-2008, the time frame of the events relevant to this case – caused the periodic starvation of children. The Ethiopian military forces that had been invited by the TFG to protect it intermittently fought a civil war which killed thousands of combatants and countless more civilians. (4RT 577.).

---

10 *See* http://www.enoughproject.org/files/Somalia%20After%20the%20Ethiopian%20Occupation.pdf. Menkhaus, the author, is an Associate Professor of Political Science at Davidson College.

Thus, for nearly two decades prior to the time frame of this case, Somalia existed in the state of nature described by Thomas Hobbes—"continual fear and danger of violent death; and the life of man, solitary, poor, nasty, brutish and short." Leviathan, pt. i, ch. 13 (1651). Indeed, in 2008, after lacking a central government since 1991, Somalia began its six-year run as the number one failed state on earth. *See* https://en.wikipedia.org/wiki/List_of_countries_by_Fragile_States_Index.

The Appellants, all emigres from Somalia during this period of crisis there, are part of the worldwide Somali diaspora that diligently monitors events in their homeland, including the impact of the Ethiopian invasion of Somalia, the death and displacement of hundreds of thousands of Somalis at the hands of Ethiopians, as well as famine and drought that have plagued Somalia and its inhabitants, particularly children. According to Bryden, the Somali diaspora has been a critical source of political and financial support for activities in Somalia, sending between $500 million and $1 billion back to their homeland every year. Links between the diaspora and Somalia itself are very active. (4RT 582.)

C. Pre-Trial Proceedings: Motions to Suppress and Access to Exculpatory Evidence

In their pretrial motions, defendants sought, *inter alia*, (1) suppression of the fruits of the electronic surveillance conducted pursuant to FISA; (b) disclosure of

exculpatory material and information; and (3) an order, pursuant to Federal Rule of Criminal Procedure 15, directing depositions of certain witnesses located outside the United States. (CR 92; 154.) As detailed below, the district court denied the first motion, deferred to the government with respect to the second motion, and granted in part the third motion.

1. Defendants' Pre-Trial Motions to Suppress the Fruits of the Eavesdropping Conducted Pursuant to the Foreign Intelligence Surveillance Act ("FISA").

The first two arguments of this brief were raised before the district court[11] in their initial pretrial motions defendants moved to "suppress all interceptions made and electronic surveillance conducted pursuant to the Foreign Intelligence Surveillance Act (hereinafter "FISA"), 50 U.S.C. §1801, *et seq*., and any fruits thereof, and/or for disclosure of the underlying applications for FISA warrants, and/or an evidentiary hearing on the issues, because the FISA surveillance was obtained and conducted in violation of FISA and the First and Fourth Amendments to the U.S. Constitution[.]" (CR 92, Def. Mtn. to Suppress); (CR 345, Def. Mtn. New Trial.)

The district court denied that motion without conducting an evidentiary hearing or providing defendants' counsel access to the documents underlying the FISA

---

11 Some factual allegations are particularly relevant to either the statutory or the constitutional challenge, but not both. Those facts will be set forth in the argument sections in order to avoid repetition.

applications and orders (including redacted *ex parte* portions of the government's response to the motion). (CR 124, suppression denial; CR 386, denying new trial.)

2. Defendants' Motions for Disclosure of Exculpatory Material and Information.

In their pretrial motions, defendants moved for production of exculpatory material the government was obligated to provide under *Brady v. Maryland*, 373 U.S. 83 (1963), and its progeny. (CR 92, at 34-36.) In large part, the specifics of the motion were based on a June 15, 2011, FBI San Diego Field Intelligence Group Assessment (hereinafter "FIG Assessment").

That FIG Assessment was summarized in a two-page partially redacted FBI Report dated June 15, 2011, created by the San Diego office (denominated in discovery as GA-DOCS-000051-52, and as Exhibit 1 to CR 92). *Id.*

According to the FIG Assessment:

> [t]he San Diego FIG assesses that Moalin, who belongs to the Hawiye tribe/Habr Gedir clan/Ayr subclan, is the most significant al-Shabaab fundraiser in the San Diego Area of Operations (AOR). Although Moalin has previously expressed support for al-Shabaab, he is likely more attentive to Ayr subclan issues and is not ideologically driven to support al-Shabaab. The San Deigo FIG assesses that Moalin likely supported now deceased senior al-Shabaab leader Aden Hashi Ayrow due to Ayrow's tribal affiliation with the Hawiye tribe/Habr Gedir clan/Ayr subclan rather than his position in al-Shabaab. Moalin has also worked diligently to support Ayr issues to promote his own status with Habr Gedir elders. The San Diego FIG assesses, based on reporting that Moalin has provided direction regarding financial accounts to be used

> when transferring funds overseas that he also serves as a controller for the US-based al-Shabaab fundraising network.

Id.

Defendants' motion for *Brady* material also referenced prior investigations of Moalin, and sought exculpatory information and material regarding them as well, and/or an order compelling the government to produce such information, in particular that referenced in the FIG Assessment. (CR 92, at 34-36.)

The district court denied that motion as well, relying on its confidence in the government's adherence to its obligations under *Brady*. (CR 146.)

3. Defendants' Motions for Depositions Pursuant to Federal Rule of Criminal Procedure 15.

Prior to trial, defendants moved pursuant to Rule 15 for depositions of certain defense witnesses located overseas. The witnesses resided in Somalia, or elsewhere in Africa, and either could not, or would not, travel to the U.S. to testify at trial. Following some discussion and negotiation, the Court granted the motion to the extent the depositions could be conducted in Djibouti (due to safety considerations with respect to Somalia.)

However, with respect to one potential deponee, Farah Shidane, a/k/a "Farah Yare," a Djibouti national as well as an unindicted co-conspirator, the government wrote Ahmed Taalil's counsel October 11, 2012, that

> [a]fter some reflection, we determined we are not in a position to give any assurances to the deponents as to safe passage out of Djibouti. Our understanding is that they are voluntarily appearing there at the depositions. We do not know much about them, or what they are going to say, and, as we informed you and the court, one of them is an uncharged co-conspirator.

(CR 213-2 at 2.)

In addition, in a telephone conversation Friday, October 12, 2012, with counsel for Nasir Mohamud and counsel for M. Mohamud, the government asserted that "[o]ne way or another, [the witnesses] have a personal interest to consider if they have liability[,]" and that if certain of the witnesses (whom he did not identify further) testified in their deposition(s) consistent with their proffered testimony (in the Rule 15 motion papers), "they wouldn't be telling the truth." (*Id.*)

The government further stated that under those circumstances, while there "is no arrest warrant or secret indictment out there" (with the exception of the one witness who is also an unindicted co-conspirator) the government could not guarantee the U.S. government "wouldn't do something while [the witnesses] are there [in Djibouti]." The Assistant United States Attorney added that he also "wanted to keep [his] options open[,]" reiterating his belief that "[s]ome of [the witnesses] have liability," and that "they should get their own lawyer." (*Id.*)

As a result, and in light of Shidane's status as an alleged co-conspirator and his

consequent potential liability, defense counsel had requested "safe passage" from Djibouti for Shidane, or, at least, a written representation that the government would not seek to issue process against any of the defense witnesses while they were in Djibouti. Counsel first raised this issue with the government in a meeting on August 21, 2012.

Indeed, because the government had earlier indicated it would seek safe passage for the witnesses if they were willing to come to the United States, counsel also went so far as to provide sample "safe passage" letters (provided in other cases for defense witnesses, including potential co-conspirators) to the government at that meeting. (CR 213-2 at 3.)

In addition, during the August 21, 2012, chambers conference with the Magistrate Judge to whom the district court delegated the logistical preparation for the Rule 15 depositions (and who ultimately presided over the depositions in Djibouti) the government represented that it would facilitate safe passage to the U.S. in an effort to secure the witnesses' presence and testimony at trial (rather than via Rule 15 depositions conducted overseas). In subsequent telephone conversations, that government position had been reiterated to defense counsel. (CR 213-2 at 3-4.)

Yet the government refused to provide safe passage, which became an issue only with respect to Shidane. As a result, the defense moved to compel the

government to provide safe passage, and that the government's failure to do so violated the Sixth Amendment right to present their defense.

Ultimately, Shidane refused to travel to Djibouti and expose himself to arrest by either Djibouti or U.S. authorities. As a result, the defense was unable to conduct his deposition. Shidane was mentioned often at trial, was a party to several of the intercepted conversations introduced in evidence, was the alleged destination of certain funds transmitted in the case and alleged in the Superseding Indictment, and was the subject of a stipulation – Defense Exhibit 4 – that stated that "in early to mid-2008[,]" (1) "individuals including [Shidane] were associated with the Ilyas charity[;]" (2) "[m]oney collected by the men in [the pertinent locale in Somalia] on behalf of the Ayr sub-clan was given to a group that was not al-Shabaab[;]" (3) "[t]here was a dispute between al-Shabaab, the Ayr clan, and Ilyas over the administration of the [pertinent] regions[;]" and (4) "[m]embers of the Ilyas charity . . . were opposed to al-Shabaab and were Ayrow's enemies." (12RT 1732-33.) Nor did the government, at trial, introduce any evidence with respect to Shidane other than the intercepted telephone calls to which he was a party. (Gov. Exhibits 182, 191; 6RT 1090, 7RT 1180.)

D. The Trial

Trial lasted four weeks, three of which were devoted to the evidentiary

presentation. The government called twelve witnesses, while the defense called ten. Both sides introduced tapes and transcripts from the conversations intercepted pursuant to FISA, as well as other documents and records. In addition, the defense introduced a stipulation regarding certain events and relationships in Somalia.

1. Government's Core Evidence

The government relied predominantly on the telephone conversations intercepted pursuant to FISA. Indeed, the government did not call a single witness who had ever met any of the defendants. Rather, the government's evidence was admitted through an expert, FBI agents (including a linguist), and a records custodian for the company that had acquired the Shidaal *hawala*.

The FISA Orders were for electronic surveillance of Moalin's telephone, but conversations for all four defendants were intercepted during the course of the nearly nine-month FISA wiretapping. All involved Moalin as one of the parties to the conversation(s). The government argued that another party to a number of those conversations, a person calling himself "Sheikalow," was in fact Aden Ayrow, a principal al-Shabaab military commander.

The government did not present any evidence (a) identifying Ayrow's voice on the tapes, either through a witness or any scientific method or comparison; (b) identifying any telephone numbers associated with Ayrow; (c) that Ayrow had any

nicknames, much less "Sheikalow;" (d) that Moalin (or any of the other defendants) knew Ayrow; (e) that Ayrow received any of the money transmitted by the defendants; and/or (f) that any of the references on the telephone conversations were personal to Ayrow, and/or identified him by some specific piece of information.

The government's theory of the prosecution was that until at least August 5, 2008, the defendants conspired together and with others to provide money to al-Shabaab and others engaged in violent attacks on the TFG and its supporters. The government asserted that the telephone conversations intercepted pursuant to FISA established the defendants' provision of material support to Aden Ayrow, al-Shabaab, and others engaged in killing and the use of weapons of mass destruction in Somalia.

According to the government, these intercepts included numerous conversations between Moalin and Aden Ayrow, who typically used the code names "Shikhalow" and "Majadhub." The government also introduced transaction records from Shidaal Express documenting the money transfers discussed in the recorded conversations.

Regarding the intercepted telephone conversations, the government concentrated on the following calls (which were translated from Somali and transcribed): In December 2007, "Sheikalow" told Moalin that he needed more than $3,000 for his forces in the Bay and Bakool regions of Somalia. Sheikalow told

Moalin to call the "cleric" [allegedly Mohamed] immediately about the matter. Moalin stated that he would "take care of the issue swiftly" with "the cleric" and "the Saleban clan cleric whom you talked to, by the name of Sheikh Issa." (Gov. Exhibit 120; 5RT 990.)

Moalin immediately called Doreh, informing him that the "cleric" just called and requested money for the forces stationed where the fighting is occurring. Moalin urged Doreh to contact Mohamed. The next day, Moalin told Ahmed Taalil that "the young men who are firing the bullets" need money, that these men are "the strongest men after those in Mogadishu," and that they killed 60 Ethiopians and destroyed up to five vehicles in just the previous month. (Gov. Exhibit 123; 5RT 1007.)

Moalin advised Nasir Mohamud they needed money for the forces "doing that job." Nasir Mohamud indicated he would look for it. Moalin told M. Mohamed in a December 28, 2007, telephone conversation that the men have been "crying out to me over the phone." M. Mohamed stated that he would "complete the task" pertaining to the men. (Gov. Exhibit 124; 7RT 1233.)

In a January 1, 2008, recorded conversation, Moalin told Sheikalow that a "small amount" had been sent to him under the name "Yusuf Mohamed Ali." Sheikalow then reported that "these two nights we gave the non-Muslims a holiday

to remember."[12] Laughing, Moalin observed that if those attacked had been Somali, they would have known where to run, but instead "they have to die because they don't know where to run to." (Gov. Exhibit 120; 6RT 1013-14.)

The Shidaal Express records introduced by the government reflected that January 1, 2008, two transfers of $1,950 (totaling $3,900) were sent from San Diego to "Yusuf Mohamed Ali" in Mogadishu. (Gov. Exhibit 39; 5RT 825.)

Two days later, Sheikalow told Moalin that "we received the three." Also that day, January 3, 2008, Moalin afforded Sheikalow access to his house – the government claimed the reference was to Moalin's house in Mogadishu, while the defense's position that it referred to Moalin's house in Guracel. Moalin provided Sheikalow detailed instructions to the house, and told Sheikalow that "you can use it for anything you want – I mean – if you want to hide stuff in there." (Gov. Exhibit 131; 5RT 860, 863, 6RT 1080.)

Moalin told Sheikalow that Sheikalow could bury his "stuff" deep in the ground and then plant trees on top. Moalin told Sheikalow he would have trees brought over from a farm for that purpose. Moalin also informed Sheikalow that the house has an attic where he used to store documents and weapons. Moalin added that

---

12 While Ethiopia is predominantly a Christian country, there was a dispute at trial regarding the precise meaning of the term – whether it meant "non-Muslim" or Ethiopians generally.

the house's only drawback was that it is "easily identifiable" and an "easy target" because of its location and trees. (*Id*.)

Sheikalow, however, shrugged off that concern, responding, "No one would know. How could anyone know, if the house is used only during the nights?" (*Id*.) A few days later, Moalin told Nasir Mohamud that the "young men" had created an efficient structure to fight against the police, the tax collectors, and the upper administration, and that the "situation" is in a "very good phase." Moalin stated that "you can sense that" from the fact that "up to eight tax collectors were killed the other day" and "the continuous attacks against the camps, you know, never stopped." (Gov Exhibit 133; 6RT 1017.)

Moalin, in a January 20, 2008, conversation, advised Sheikalow to focus on "military" matters, but to allow clan members in the Guriceel area to establish a local administration and handle "the overall politics." Sheikalow replied that, in Islam, "politics and military go together" and that "Islam has its own political principles" where "the fighter, the politician and the missionary must all come together in a single unit." According to the government translation, Sheikalow added that "And we, the Shabaab, have a political section, a military section and a missionary section. We have all that." (Gov. Exhibit 131; 6RT 1019.)

During that same conversation, Sheikalow told Moalin that "[t]he other day,

we planted a land mine for Abdi Qaybdiid [Mogadishu police commissioner] who was traveling on that road; he was almost hit." Sheikalow told Moalin to tell "Sheikh Mohamed" that "he must let us know the amount of money we can expect every month, even if it is one hundred dollars." Sheikalow stated, "We want to support the insurgent with it." (Gov. Exhibit 136; 7RT 1208.)

Sheikalow then told Moalin that the TFG's Nur Adde and Ahmed Abdisalan (the TFG's Prime Minister and Deputy Prime Minister) "arrived today" and that "as soon as they arrived at the Presidential Palace, we hit them with 12 mortar shells." Sheikalow observed that Villa Somalia (the Presidential Palace) "is still full of smoke." Moalin replied, "God is great. God is great. It is something to be thankful of the fact that you are capable to deny them the opening of new offices and to work as a functioning government." (Gov. Exhibit 131; 6RT 1019.)

Sheikalow asked Moalin in a February 3, 2008, conversation if Moalin had reached "Sheikh Mohamed." Sheikalow stated, "You are running late with the stuff. Send some and something will happen." Moalin subsequently asked Doreh February 9, 2008, if the money held by "Mohamed Khadar" had been sent. Doreh replied affirmatively, noting that "the Dhunkaal one" had been sent. (Gov. Exhibit 140; 5RT 870.) On February 13, 2008, Mohamed told Moalin he believed "Dhunkal was able to get the stuff there." (Gov. Exhibit 139; 6RT 1022.)

The next day, Moalin asked Sheikalow, "Did you receive Dhunkaal's stuff?" Sheikalow asked Moalin whether he used the name "Yusuf Mohamed Ali as the receiver." Moalin replied affirmatively, telling Sheikalow that the amount was "2,000." (Gov. Exhibit 143; 6RT 1037.) The Shidaal Express records reflect that February 13, 2008, two transfers totaling $2,000 ($1,300 and $700) were sent from San Diego to "Yusuf Mohamed Ali" in Dhusamareeb, Somalia. The sender was listed as "dhunkaal warfaa." (Gov. Exhibit 39; 7RT 1158.)

On March 30, 2008, Sheikalow told Moalin to "tell Sheikh Mohamed that we are waiting news from him and news from you." Moalin indicated they were trying, but the situation was difficult because of the drought. (Gov. Exhibit 149; 6RT 1044.) On April 12, 2008, Sheikalow told Moalin that "[i]t rained everywhere" and "the water tanks are full." Sheikalow stated, "The help for the drought is over; so now it is the time to finance the jihad." Sheikalw told Moalin that the Ethiopians were in Adaado (near Dhusamareeb), and Moalin replied, "I was told they are only a few men so why do you not prepare to finish them off?" Sheikalow answered, "We will try, God willing." (Gov. Exhibit 151; 6RT 1047.)

On April 12, 2008, Sheikalow again urged Moalin to provide money, stating that he didn't believe that even 200 men "will have bullets to shoot at the enemy they can see" but "if we had bullets for this enemy we would have destroyed them."

Moalin replied that he would do his best. Within less than an hour, Moalin told M. Mohamed that he had received calls "from the young man" who stated that "he does not have anything to throw at them." M. Mohamed stated that it is "best that this thing does not become public." (Gov. Exhibit 153; 6RT 1051-52.)

On April 17, 2008, Moalin spoke with M. Mohamed again, asking whether they could commit to a date to provide Sheikalow funds. M. Mohamed asked Moalin whether he and "the others" had any money. M. Mohamed told Moalin that they would meet concerning the matter. Moalin suggested that M. Mohamed to hold back twenty or thirty trusted people at the Mosque on Friday and "tell them to pay this much, something they can afford." (Gov. Exhibit 155; 6RT 1056.)

On April 23, 2008, Moalin asked M. Mohamed whether "Dhunkaal" left. M. Mohamed replied, "Dhunkaal left. Dhunkaal left." However, Mohamed could not recall the name under which the funds had been sent, stating that he had left the paper at home. Mohamed called Doreh at Shidaal Express, who told him that the funds were sent from "Abdiweli Ahmed" to "Dhunkaal Mohamed Yusuf." (Gov. Exhibit 158; 6RT 1059.)

In an April 24, 2008, conversation, M. Moalin asked Sheikalow if he had "received the little that we sent you." M. Moalin told Sheikalow that the transfer "was sent from San Diego directed to Dhunkaal." Moalin added that the transfer was "three

bundles [$3,000]" but "[t]hey will break it because they do not want to show that the transfer was one." (Gov. Exhibit 161; 6RT 1062.)

The next day, April 25, 2008, Sheikalow told Moalin that he had received "1,900." Less than an hour later, Moalin asked M. Mohamed, "how many stones did we send him?" M. Mohamed replied, "It was three stones [$3,000]." Moalin stated, "Yes, naturally they sent it in installments." Moalin then called Sheikalow and told him that the entire transfer was "three stones" but was structured, so if that Sheikalow had received "19" [$1,900], he should go look for the rest. Moalin also told Sheikalow that Doreh helps them by waiving the typical hawala transfer fee. (Gov. Exhibit 164; 7RT 1214.)

The Shidaal Express records reflect that, on April 23, 2008, two transfers totaling $3,000 ($1,900 and $1,100) were sent from San Diego to "Dunkaal Mohamed Yusuf" and "Mohamed Yusuf dunkaal," respectively, in Dhusamareeb. (Gov. Exhibit 39; 6RT 1061.)

Aden Ayrow was killed in Somalia by a U.S. cruise missile strike May 1, 2008. The government did not offer any details about where and how, or precisely when, Ayrow was killed. In a May 1, 2008, conversation, Moalin was informed that "birds targeted the house where Sheikalow, 'Slim Limbs', used to stay one hour ago." ((Gov. Exhibit; 7RT 1169.)

Later that morning, Moalin asked another person if he had "information about Dhusamareeb. Was there a plane attack today?" That person replied, "I don't know the exact time but last night an airplane dropped a missile on a house of three bedroom thought to be inhabited by the main man." Approximately an hour later, Moalin contacted M. Mohamed, stating, "Naturally, I think you have heard what happened." M. Mohamed replied, "Man, I am sitting in front of it and looking at it right now." (Gov. Exhibit 170; 6RT 1067-68.)

Subsequently, in a July 10, 2008, conversation, Moalin informed Nasir Mohamud that they had collected about $10,000 "including from the mosque." Moalin stated that they "sent $5,000 as emergency to the men involved in the fighting in the Galgadud region." Moalin explained that they would divide the $5,000 between the "men from the Youth" and another group known as "Jabiso." (Gov. Exhibit 186; 7RT 1174.) Shidaal Express records indicate that $5,000 was sent in a series of transfers to Farah Shidane. (Gov. Exhibit 39; 7RT 1181.)

On July 11, 2008, Moalin spoke with Mahad Karate, who told Moalin to send funds directly to a man named Omar Mataan. (Gov. Exhibit 187; 7RT 1227.) Later that day, Moalin spoke with Omar Mataan. Mataan stated that he was in Dhusamareeb. Moalin told Mataan that he would use the name "Dhunkaal" to send the funds. (Gov. Exhibit 188; 7RT 1227-28.)

On July 17, 2008, Moalin told the owner of the Shidaal Express that he wanted to send the "two cartons" [$2,000] discussed with Sheikh Issa. (Gov. Exhibit 192; 7RT 1230.) On July 22, 2008, Moalin told Omar Mataan that "we threw two cartons addressed to you" to Dhusamareeb. (Gov. Exhibit; 7RT 1186.) The next day, Moalin asked Sheikh Issa to "keep an eye" on the "two cartons" allocated for "the youngsters." (Gov. Exhibit 198; 7RT 1186-87.)

The Shidaal Express records reflect that July 23, 2008, two transfers totaling $2,000 ($1,650 and $350) were sent from San Diego to "Omer Mataan" and "Omer matan," respectively, in Dhusamareb. (Gov. Exhibit 39; 7RT 1187.)

2. The Defense Case

Defendants did not dispute that they sent money to Somalia. Defendants did not dispute that Moalin (and at times, the other defendants) engaged in telephone conversations with persons in Somalia. Defendants did not contest that they were deeply concerned with events and developments in their perpetually conflict-ridden homeland. Nor did they contest that those recorded conversations included their frank, emotional, and often spontaneous expression of opinion about politics, government, and internal affairs in Somalia.

However, defendants denied that the money they transmitted to Somalia was intended for al-Shabaab, or the benefit of al-Shabaab. Rather, their intention was to

assist the fragile local administration that governed the Gelgaduud region of Somalia, including the city of Guracel, and provide aid for drought relief, schooling for children, particularly orphans and girls, and security against both banditry and the predations of al-Shabaab.

Defendants presented that case through six witnesses who testified via video depositions conducted pretrial in Djibouti, another two Somali witnesses who testified at trial (in addition to a Somali linguist and an investigator), cross-examination of government witnesses (in particular, the government's expert and its Somali linguist), documents and photographs, and a Stipulation with respect to certain antagonistic relationships in Somalia between Aden Ayrow and the defense witnesses (and the organizations in Somalia with which they were affiliated, and to which Moalin contributed money and other aid), as well as with Farah Shidane, who was overheard on some of the telephone conversations. (Gov. Exhibits 182, 190; 6RT 1090; 7RT 1177); (12RT 1732-33.)

All of the defense's eight fact witnesses were personally acquainted with Moalin, either in the U.S. or (more commonly) in Somalia. For example, Halima Yare, who testified at trial and had been targeted by al-Shabaab, was familiar with Moalin as a result of his (and her) charitable work in Galgaduud and Guracel, and Moalin's abiding interest in the welfare of those areas in Somalia, including through

the ILAYS Foundation, a local Somali charity. (10RT 1438.) Al-Shabaab was opposed to IIDA as an idea, but they did not have the power to stop it. They put her on the list of people that they are killing because she did these schools (for girls in the Galgaduud region in 2007 and 2008.) She also testified with respect to Farah Shidane, his work on behalf of the communities in Gelgaduud and Guracel, particularly with respect to drought relief and infrastructural construction, and his political affiliations, which did not include any affinity with al-Shabaab. (10RT 1454.) (In fact, the antipathy between Farah Shidane and al-Shabaab was confirmed by the Stipulation introduced at trial. (12RT 1732-33.)

Similarly, Abdisalem Guled, at the time of his testimony the national security adviser to the President of Somalia, (12RT 1671), testified of his direct knowledge of and interaction with Moalin in the context of Moalin's charitable and civic work on behalf of Somalis in Guraceel and the Gelgaduud region. (12RT 1709.)

Six other defense witnesses – Abukar Dahir Mohamed (a/k/a "Abukar Suryare"), Hassan Guled (a/k/a "Sheikalow" or "Hassan Yare"), Sheik Abdur Rahman (a/k/a "Gido Quorow"), Osman Nur, Najib Mohammad, and Sharif Qorey – testified via their video depositions that had been conducted prior to trial in Djibouti pursuant to Rule 15. (11RT 1596-97, 1607, 1630).

All six witnesses testified to their personal contacts with Moalin. Najib

Mohammad, a telephone operator who connected Moalin with persons in Somalia, testified that his discussions with Moalin included informing Moalin of news from Somalia, including political and other developments and events. (5RT 941, 6RT 1011, 1057, 7RT 1168; 8RT 1309.) He did not have any information to suggest that the "Sheikalow" with whom he connected Moalin was Aden Ayrow, or anyone connected with al-Shabaab. (9RT 1408, 11RT 1596, 12RT 1732-33.)

The other five witnesses testified with respect to their personal knowledge of Moalin's humanitarian and charitable endeavors in Gelgaduud and Guracel, including financially supporting schools (particularly for girls), orphanages, drought relief projects, and security, and Moalin's affiliation with the ILAYS Foundation. They also testified to Farah Shidane's connection with the ILAYS Foundation.

In addition, Messrs. Dahir Mohamed, Abdur Rahman, and Nur were officials in the regional governmental administration in Guracel, and in that capacity were responsible for the area's defense against both al-Shabaab and the Ethiopian military. (9RT 1408, 11RT 1596.) They also testified with respect to Farah Shidane's lack of any affiliation with al-Shabaab; in fact, they testified that they all, including Farah Shidane, were opponents of al-Shabaab, which was subsequently verified by the Stipulation between the parties. (12RT 1732-33.)

Abdur Rahman also testified that Moalin's wife was Abdur Rahman's sister,

and that she and Abdur Rahman were adherents of *sufi* Islam, an anathema to al-Shabaab. (*cf*. 4RT 629.) Abdur Rahman and Nur also described how they fought in armed clashes with al-Shabaab. Nur and Abdur Rahman were also members of an Islamic organization in Somalia, *Ahlu Suna Wa Jameea*, that was engaged in open and armed conflict with al-Shabaab, and ultimately drove al-Shabaab from Guracel.

Hasan Guled, police commissioner in that regional administration in Guracel, testified that he went by the nickname "Sheikalow," had engaged in telephone conversations with Moalin during the time period of the FISA interceptions about many of the subject matters that were discussed during the recorded conversations between Moalin and "Sheikalow," including orphanages involving a person named Salah, Moalin allowing Guled's police force to use Moalin's house in Guracel as a station, and other events occurring in the area. (12RT 1728.)

Hasan Guled also testified that he fled the area (and sought refuge in Ethiopia) after Aden Ayrow was killed because al-Shabaab blamed the regional administration for providing the U.S. with Ayrow's whereabouts, and attacked the police and the regional administration in Guracel. As a result, he did not speak to Moalin after Ayrow was killed, and stayed in Ethiopia for an extended period. (*Id*.)

Defendants also admitted portions of certain intercepted conversations that had been introduced by the government (but which did not include the entirety of the

conversation), as well as portions of or entire conversations not offered by the government at all.

In connection with the tape recordings, the defense called Abdi G. Elmi, a certified Somali translator, (10RT 1483), and Christopher Chang, an investigator who introduced certain defense exhibits and presented the transcripts of the conversations introduced by the defense. (8RT 1335.) In particular, Elmi testified with respect to the context in which Moalin and "Sheikalow" used the term "shabaab" and "shabaabka" during their telephone conversations. (8RT 1343.)

The defense offered additional evidence of Moalin's opposition to al-Shabaab, through testimony and other evidence, but, as detailed in argument IV, the district court precluded such evidence because it referred to events occurring after the period specified in the Superseding Indictment.

At the conclusion of the defense case, a Stipulation was admitted by the defense as a result of the processes attendant to the Classified Information Procedures Act ("CIPA"). The content of the Stipulation, marked as Court Exhibit 4, (12RT 1734), read in its entirety as follows:

"in early to mid 2008,

(1) money collected for the Ayr sub-clan was given to individuals, including Abukar Suryare (Abukar Mohamed), and Fare Yare, who were associated with the ILAYS charity;

(2) money colleted by men in Guracewl on behalf of the Ayr sub-clan was given to a group that was not al-Shabaab;

(3) there was a dispute between al-Shabaab, the Ayr clan, and ILAYS over the administration of the Galgaduud region; and

(4) members of the ILAYS charity and the Ayr sub-clan, including Abukar Suryare, were opposed to al-Shabaab and were Ayrow's enemies."

(12RT 1732-1733.)

3. The Verdict

The jury convicted all four defendants on all counts in which they were charged, respectively, in a verdict returned February 22, 2013. (CR 303.)

E. Post-Trial Disclosures by U.S. Government Officials Regarding the Interception/Collection of Moalin's Electronic Communications

As detailed in arguments I and II, in June 2013 U.S. government officials, in response to disclosures by Edward Snowden regarding the National Security Agency's bulk collection of the telephone metadata involved in essentially *all* U.S. domestic calls, revealed that such collection, retention, aggregation, and utilization of Moalin's telephone metadata had been the catalyst for the investigation of Moalin. Those officials also revealed that there had been an earlier 2003 investigation of Moalin that had not yielded any connection with terrorist activity.

As a result, defendants moved post-trial for an evidentiary hearing, suppression of the FISA intercepts (and any other fruits of the telephone metadata collection), a

new trial, and/or disclosure of *Brady* material that had previously been withheld. (CR 345.) The district court denied those motions without an evidentiary hearing in an opinion issued November 18, 2013. (CR 386.)

F. Sentencing

At sentencing, the district court noted that "[w]hen it comes to specific deterrence I don't think we need worry about any of these three gentlemen." (Sent. Trans. at 130; *id*., at 52-54 (Moalin's charitable works); at 92-94 (Mohamud's good works); at 129-30 (same regarding Doreh.)[13]

Ultimately, the district court imposed the following custodial sentences upon the four defendants:

Moalin	18 years
M. Mohamud	13 years
Doreh	10 years
Nasir Mohamud	6 years

Regarding Moalin's sentence, the district court imposed a sentence of 15 years' imprisonment on Counts 1, 2,3, and 5 to run concurrently, and a 15-year prison sentence – three of which were to run *consecutively* to other sentence(s) – on Count

---

13 While the district court was referring specifically to Moalin, Mohamud, and Doreh, that was because only those three defendants were sentenced that day (because of the unavailability of Ahmed Taalil's counsel). There is no reason to believe the district court held any different opinion with respect to Ahmed Taalil Mohamud, sentenced two months later, as he received the shortest term.

4. (CR 392.) All of the other sentences for the other defendants were imposed concurrently. (CR 393-394, 431.)

SUMMARY OF ARGUMENT

Appellants' first two arguments are about the constitutionality of the NSA's bulk metadata collection program and whether the NSA bulk collected the data in violation of the enabling statute. Metadata can tell you a person's daily routines and private habits. The government's collection and retention of this data for use in investigation presents a grave danger to personal privacy. Personal details of private life can be deduced from a person's calling patterns. Disturbingly, both the government and the district court found that Appellants have no privacy interest whatsoever in their telephony metadata based upon pre-internet cases in which land-line telephones were the subject under inquiry. In those cases, there was never a concern about the government agglomerating evidence about what the entire populace does and using it to investigate and prosecute criminal cases. The difference between the government being able to search all the cellular phone records of everyone in bulk collection is not just a difference in degree, it is a difference in kind. The telephony metadata presents a grave threat to the privacy interests of individuals protected by the Constitution. If the government is allowed to collect and utilize bulk data to prosecute us, there is a severe danger that the government will put that data to other

uses. Put differently, the constitution does not allow the government to set up a surveillance state in which it monitors our every move.

Appellants' first argument asks this Court to follow the lead of the Second Circuit in *Clapper* and find that it does not need to reach the constitutional claims because the enabling statute for the bulk metadata collection did not authorize the wholesale procurement of everyone's metadata. Constitutional avoidance counsels interpreting statutes to avoid the unconstitutional applications if possible and the Second Circuit convincingly explained why that doctrine is particularly apropos with respect to the NSA's bulk metadata collection program.

If the Court concludes that the NSA was authorized by the statute to seize and maintain bulk telephony metadata, then Appellants believe that the statute violates the constitution. Secret and mass surveillance is the hallmark of a police state and is antithetical to values of individual privacy and freedom protected by the United States Constitution.

Appellants' third argument regards the provision of *Brady* material. In 2002, the government conducted an investigation of Moalin in which it concluded that he was not involved in terrorism and instead was a supporter of his clan. This evidence was have supported Moalin's argument that he was not a supporter of al-Shabaab and its exclusion violated his right to present a defense.

The results of the 2002 investigation would have cohered with Moalin's activities in arranging the peace/women's right conferences. The district court found that because these activities occurred after the time-frame charged in the indictment, they were not relevant. But the point of the evidence was to show that Moalin was not just unaligned with al-Shabaab, but that he had such different beliefs that he never would have knowingly supported the terrorist organization. The nature of the relevant beliefs – i.e. whether Moalin is a supporter of militant fundamentalist Islam – are deep, core beliefs and not the kind that one would expect to vary since deviation from the code of fundamentalist Islam is apostasy and is punished by death.[14]

Appellants also wanted to present the testimony of Farah Shidane. The district court refused to either make the government give Shidane safe passage or to allow for his videotaped deposition. Shidane's testimony would have directly contradicted the government's theory, a point essentially conceded by the government when it argued that it believed that Shidane's proffered testimony would be false.

Contrasted to the preclusion of Appellants' exculpatory evidence about what beliefs they held was the district court's allowance of the "Black Hawk Down" evidence. This evidence implicitly sent the message that the United States had enemies in Somalia and it does not take an advanced degree to figure which roles

---

14 *See, e.g., Bastanipour v. INS*, 980 F.2d 1129, 1133 (7th Cir. 1992).

were being assigned to Appellants inasmuch as they were charged with supporting the outlawed al-Shabaab, enemy of the United States.

Appellants believe that the individual evidentiary errors merit reversal individually and they also merit reversal under the cumulative error doctrine since the government's case was unfairly enhanced while Appellants evidence was unfairly restricted.

Finally, Doreh argues that the evidence against him is insufficient as it fails to show that he had any knowledge of the purpose of the transactions.

STANDARDS OF REVIEW

Motions to suppress are reviewed de novo. *See United States v. Forrester*, 512 F.3d 500, 506 (9th Cir. 2008) ("Conclusions of law underlying the denial of a motion to suppress evidence are also reviewed de novo.") The trial court's factual findings are reviewed for clear error. *See United States v.* , 497 F.3d 955, 958 (9th Cir. 2007).

This Court reviews de novo the district court's construction or interpretation of a statute." *United States v. Carranza*, 289 F.3d 634, 642 (9th Cir. 2002).

Challenges to convictions based on alleged *Brady* violations are reviewed de novo. *See United States v. Ross*, 372 F.3d 1097, 1107 (9th Cir. 2004). A district court's denial of a motion for mistrial or new trial based on an alleged *Brady* violation is also reviewed de novo. *See United States v. Antonakeas*, 255 F.3d 714,

725 (9th Cir. 2001).

A trial court's decision to admit or exclude evidence is reviewed for an abuse of discretion. *United States v. Santini*, 656 F.3d 1075, 1077 (9th Cir. 2011) (per curiam). Determination of the correct legal rule to apply is a legal question reviewed de novo. *United States v. Angwin*, 271 F.3d 786, 798 (9th Cir. 2001). The district court abuses its discretion by applying an incorrect legal rule or by applying the correct legal rule in a way that was illogical, implausible, without evidentiary support from the facts in the record, or where the reviewing court has "a definite and firm conviction that the district court committed a clear error of judgment." *United States v. Hinkson*, 585 F.3d 1247, 1262 (9th Cir. 2009) (en banc). This Court reviews de novo whether an evidentiary error rises to the level of a constitutional violation. *United States v. Pineda-Doval*, 614 F.3d 1019, 1032 (9th Cir. 2010) (citation omitted).

The district court's balancing under Rule 403 of the probative value of evidence against its prejudicial effect is reviewed for an abuse of discretion. *See United States v. Mitchell*, 502 F.3d 931, 967-68 (9th Cir. 2007) (affirming); *United States v. Gonzalez-Flores*, 418 F.3d 1093, 1098 (9th Cir. 2005) (reversing). When the district court does not engage in explicit balancing of the probative value of the evidence against its prejudicial effect, its determination is reviewed de novo. *See*

United States v. Moran, 493 F.3d 1002, 1012 (9th Cir. 2007).

This Court's standard of review for cumulative error is unclear. *United States v. Weatherspoon*, 410 F.3d 1142, 1151 (9th Cir. 2005) (reversing under heightened plain error review when only some error was preserved at trial, thereby avoiding deciding whether harmless error or plain error review applies to cumulative error).

Claims of insufficient evidence are reviewed de novo. *See United States v. Bennett*, 621 F.3d 1131, 1135 (9th Cir. 2010). There is sufficient evidence to support a conviction if, viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt. *See Jackson v. Virginia*, 443 U.S. 307, 319 (1979). This Court reviews *de novo* a district court's denial of a motion for judgment of acquittal. *United States v. Moses,* 496 F.3d 984, 987 (9th Cir. 2007). The denial of a Rule 29 motion for acquittal is reviewed the same as for a challenge to the sufficiency of the evidence." *United States v. Riggins*, 40 F.3d 1055, 1057 (9th Cir. 1994).

ARGUMENTS

I.

THE CONVICTIONS SHOULD BE REVERSED BECAUSE THE GOVERNMENT'S ELECTRONIC SURVEILLANCE, FROM WHICH ITS PRINCIPAL EVIDENCE WAS DERIVED, WAS GENERATED BY THE NSA'S BULK TELEPHONE METADATA COLLECTION AND RETENTION PROGRAM THAT EXCEEDED THE AUTHORITY CONFERRED BY THE GOVERNING STATUTE.

The government's collection, aggregation, retention, and review of Moalin's telephone metadata pursuant to its bulk telephone metadata program (hereinafter also "NSA program") – which began a process that generated the investigation and evidence, including the electronic surveillance conducted pursuant to FISA that constituted the predominant portion of the government's evidence at trial in this case – was unlawful because it exceeded the statutory authority granted pursuant to 50 U.S.C. §1861.

A. The NSA Program Was Essential to the Government's Case Herein, and to the Subsequent FISA Electronic Surveillance.

The vital importance of the NSA program's collection, aggregation, retention, and review of Moalin's telephone metadata to the government's evidence in this case is manifest. As government officials have stated publicly, it was stored metadata that in 2007, when compared with other information, caused the government to begin this

investigation of Moalin (after an earlier investigation, in 2003,) "did not find any connection to terrorist activity." (CR 345-3 at 18.)

As U.S. government officials have recounted, the connection yielded by the NSA query of its call records database permitted the government to apply for an eavesdropping warrant on Moalin's cellular telephone and e-mail communications pursuant to FISA, 50 U.S.C. §1801, et seq., which authorizes electronic surveillance *without* a showing of traditional probable cause that a crime is being committed, or about to be committed. Instead, FISA allows such electronic surveillance if the target is an "agent of a foreign power," 50 U.S.C. §1801(b), which includes any person who ""knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power[,]" §1801(b)(C) [or aids or abets or conspires to commit such activities, §1801(b)(E)], with a "foreign power" defined, *inter alia*, as " a group engaged in international terrorism or activities in preparation therefor[.] §1806(a)(4).

That FISA coverage of Moalin's cell phone and e-mails began in December 2007 and lasted eleven months, until November 2008. The government's evidence at trial consisted predominantly of selected portions of those calls. The government did not call a single witness with first-hand knowledge of the facts. The government's witnesses were either law enforcement agents who introduced the FISA recordings

or other physical and/or documentary evidence, records custodians, and an expert on the historic conflict in Somalia (who did not testify about the defendants in any respect).

Thus, the government relied overwhelmingly on the recordings intercepted via FISA, which were entirely dependent on the NSA program's exploitation of Moalin's telephone metadata. Without the NSA program's collection, retention, aggregation, and review of Moalin's telephone metadata, the government would not have commenced its investigation, it would not have been able to obtain permission to institute FISA surveillance, it would not have intercepted Moalin's telephone conversations, including those with Messrs. Mohamud, Doreh, and Nasir, and it would not have had sufficient evidence to indict the defendants, much less convict them. The NSA program's collection, aggregation, retention, and review of Moalin's telephone metadata was therefore *the* essential, irreplaceable domino that started the series of dominos, culminating in conviction of Moalin and his co-defendants.

B. Defendants' Pre-Trial Motions to Suppress the Fruits of the Eavesdropping Conducted Pursuant to the FISA.

In their initial pretrial motions, defendants moved to "suppress all interceptions made and electronic surveillance conducted pursuant to the FISA, 50 U.S.C. §1801, *et seq*., and any fruits thereof, and/or for disclosure of the underlying applications for

FISA warrants, and/or an evidentiary hearing on the issues, because the FISA surveillance was obtained and conducted in violation of FISA and the First and Fourth Amendments to the U.S. Constitution[.]" (CR 92.)[15]

In addition, defendants' motion recognized that the sources of the information in the FISA applications – unknown to the defense, which was not granted access to the applications or documents underlying them – could be illegitimate:

> [t]here is also the danger that the information in FISA applications, whether or not attributed to a particular source, was generated by illegal means such as warrantless wiretapping or constitutionally infirm FISA amendments that have yet to be challenged in criminal cases. In that context, the government should be compelled to disclose whether information in the FISA applications, or which was used to obtain information that appears in the applications, or was used in the investigation in this case in any fashion, originated from such illegitimate means.

(CR 92 at 16. (citing *Gelbard v. United States*, 408 U.S. 41 (1972) (in prosecution for contempt for refusal to testify, grand jury witness entitled to invoke as a defense statutory bar against use of evidence obtained via illegal wiretap as basis for

---

15 The FISA process is also entirely secret. In addition to the initial phase of obtaining the warrant (not distinct from that attendant to ordinary criminal warrants), the litigation of FISA surveillance is also *ex parte*. Neither defendants nor their counsel – even if they possess the requisite security clearance – are provided the FISA warrants or underlying applications (including the supporting affidavits). While FISA permits disclosure of those materials to defense counsel, *see* §1806(f) & §1806(g) – only one district judge has ever ordered such production, only to have that decision reversed on appeal. *See United States v. Daoud*, 755 F.3d 479 (7th Cir. 2014).

questions in grand jury)).[16]

C. Post-Trial Disclosures By U.S. Government Officials Regarding NSA Interception/Collection of Moalin's Electronic Communications.

In its June 8, 2013, edition, *The Washington Post* published the first in a continuing series of articles by a variety of news organs, including *The Guardian* and *The New York Times*, detailing disclosures by Edward Snowden, a former NSA contract employee. The documents Snowden provided revealed the existence of the scope of NSA's electronic surveillance, interception, and collection, including communications data relevant to U.S. persons.[17]

Two aspects of those revelations were particularly relevant to this case: (1) the

---

16 As a result, the defendants' motion requested that the district court . . .examine the nature, genesis, and provenance of the information in the FISA application, and compel the government to disclose whether any such information was the product of warrantless electronic surveillance (either via the [Terrorist Surveillance Program] or any other program), or of such surveillance authorized pursuant to the [FISA Amendments Act ("FAA")] (§1881a).
(CR 92 at 18.)

17 Two days earlier, June 6, 2013, *The Guardian* had published an article regarding a previously undisclosed order by the FISC, but Snowden was not cited as the source (although apparently he provided that document as well). *See* Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 6, 2013, available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. That article represented the first public disclosure of any of the documents and/or information provided by Snowden.

collection, storage, and subsequent retrospective use of telephone metadata of U.S. persons in the U.S., pursuant to Section 215 (50 U.S.C. §1861); and (2) the interception of electronic communications, particularly those with a domestic U.S. component (sending or receiving or, in some cases, entirely), pursuant to Section 702 (50 U.S.C. §1861) of the FISA Amendments Act (hereinafter "FAA").

In response to the Snowden/*Washington Post* disclosures, Congressional hearings were convened on the subject within two weeks. During a June 18, 2013, appearance before the House Permanent Select Committee on Intelligence ("HPSCI"), Sean Joyce, Deputy Director, FBI, testified regarding criminal cases that had been initiated as a result of the NSA interception/collection programs.

Initially, in his prepared remarks, Deputy Director Joyce informed the panel about a particular case he did not identify. He said with respect to that case,

> the FBI had opened an investigation shortly after 9/11. We did not have enough information nor did we find links to terrorism, so we shortly thereafter closed the investigation. However, the NSA, using the business record FISA, tipped us off that this individual had indirect contacts with a known terrorist overseas. We were able to reopen this investigation, identify additional individuals through a legal process and were able to disrupt this terrorist activity.

(CR 345-2 at 9-10.)

Later in that same session, during the question and answer period, Deputy Director Joyce confirmed that the case to which he had referred was *this* case: *United*

States v. Moalin, and that the individual who was the subject of the initial (closed) investigation, and whose phone records had been the subject of Section 215 collection and storage, was Moalin.

Asked by Rep. Mac Thornberry (R-Tex.) to describe the Moalin case further, Gen. Keith Alexander (USA), NSA's Director, deferred to Deputy Director Joyce, "because the actual guys who actually do all the work when we provide it is the FBI and get [the description] exactly right." (*Id*. at 18.)

As a result, Deputy Director Joyce explained that

> [i]t was a(n) investigation after 9/11 that the FBI conducted. We conducted that investigation and did not find any connection to terrorist activity. Several years later, under the 215 business record provision, the NSA provided us a telephone number only in San Diego that had indirect contact with an extremist outside the United States. We served legal process to identify who was the subscriber to this telephone number. We identified that individual. We were able to, under further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA Court, we were able to identify co-conspirators, and we were able to disrupt this terrorist activity.

(*Id*. at 18-19.)[18]

---

[18] *See also* Marshall Curtis Erwin and Edward C. Liu, *NSA Surveillance Leaks: Background and Issues for Congress*, Congressional Research Service, July 2, 2013, R43134, at 11, available at http://www.fas.org/sgp/crs/intel/R43134.pdf ("**Basaaly Saeed Moalin**: NSA, using phone records pursuant to *215 authorities*, provided the FBI with a phone number for an individual in San Diego who had indirect contacts with extremists overseas. The FBI identified the individual as [Moalin] and determined that he was involved in financing extremist activity in Somalia") (emphasis in original) (footnotes omitted).

Four weeks later, at a July 18, 2013, address at the Aspen Security Forum in Aspen, Colorado, Gen. Alexander repeated that same account of this case:

> . . . so from some information we got in Somalia, we saw some – we looked at a phone number, we said we know this is associated with *al Qaeda*, we looked at that phone number and we saw it touched a phone number in San Diego. And [Deputy Director] Joyce . . . was the one who said that was [Basaaly Moalin] case that they had started in 2003 but didn't have enough information to go up on. In 2007, we saw him talking to a facilitator in Somalia. We passed – all we have is the number. We don't know who it – a nine-digit number [or] ten-digit number. We pass that – I guess they're ten digits – we're going to be accurate – a 10-digit number to them. And they look at that and they go, ooh, this is [Basaaly Moalin]. They look up and said, four years ago we had a case. They reopened the case.

(CR 345-3 at 5; *see also* CR 345-4 Transcript, July 31, 2013, Black Hat USA 2013 Conference, Las Vegas, Nevada, Gen. Keith Alexander, at 3-4.)[19]

Deputy Director Joyce, appearing before the Senate Judiciary Committee on

---

[19] At the Black Hat conference (an annual cyber-professionals conclave), Gen Alexander recounted that

> we gave [the FBI the California telephone number] in 2007. In 2004, they had ordered an investigation on that individual, but did not have enough information to open a full field investigation, so they closed that investigation down. In 2007, with the number we gave them, they had enough information. They take that number, and now their portion of this is they can take a national security (clip?), find out who that number belongs to, and they found out it was Basaaly Moalin. They can then, with probable cause, get a [FISA] warrant. NSA only has the fact of a number. FBI could take that, see where it connects to, use a national security letter and the legal authorities given to them to take the next step.

(CR 345-4 at 3-4.)

July 31, 2013, reiterated during his testimony the genesis and chronology of the investigation in this case:

> another instance when we used the business record 215 program, as Chairman – Leahy mentioned, [Basaaly Moalin]. So, initially, the FBI opened a case in 2003 based on a tip. We investigated that tip. We found no nexus to terrorism and closed the case.
>
> In 2007, the NSA advised us, through the business record 215 program, that a number in San Diego was in contact with an Al-Shabaab in East Al Qaida – East – Al Qaida East Africa member in Somalia. We served legal process to identify that unidentified phone number. We identified [Moalin].

(CR 345-5: Transcript, July 31, 2013, Senate Judiciary Committee, Deputy Director Sean Joyce, at 14.)

In addition to those post-trial disclosures, the material produced pursuant to 18 U.S.C. §3500 for the government's linguist, Liban Abdirahman, included a January 24, 2008, e-mail from a redacted source (probably FBI Special Agent Michael C. Kaiser, the case agent) that stated, "We just heard from another agency that Ayrow tried to call Basaaly today, but the call didn't go through." (CR 361 at 17; *see also* CR CR 370, Sent. Memo Moalin, at 32-33.)

D. The District Court's Opinion Denying Defendants' Post-trial Motion.

In denying Defendants-Appellants' motion for a new trial pursuant to Federal Rule of Criminal Procedure 33, the district court did not address the statutory issue

at all. In its opinion, the district court instead concentrated on the constitutional question, and relied on *Smith v. Maryland*, 442 U.S. 735 (1979), for the proposition that person lacks any legitimate expectation of privacy in telephone metadata, *i.e.*, the telephone numbers dialed, and denied the motion accordingly. (CR 386; ER 61.)

The infirmities in the district court's constitutional analysis are clear in light of the Supreme Court's 2014 decision in *Riley v. California*, 573 U.S. ___, 134 S. Ct. 2473 (2014), the Second Circuit's recent decision in *ACLU v. Clapper*, and the decision of the district court in *Klayman v. Obama*, 957 F.Supp.2d 1 (D.D.C.2013), *vacated and remanded*, ___ F.3d ___, 2015 WL 5058403 (D.C. Cir. August 28, 2015) (which invalidated the NSA program on constitutional grounds but has since been vacated and remanded on standing grounds.)

E. The NSA's Telephone Metadata Collection Program Exceeded the Statutory Authority Congress Granted Pursuant to §1861.

As detailed below, with respect to the statutory violation, this past May in *ACLU v. Clapper* the Second Circuit held that NSA's telephone metadata program implemented pursuant to §1861 "exceeds the scope of what Congress has authorized[.]" 785 F.3d at 826. The Circuit characterized the NSA program as an "unprecedented and unwarranted" interpretation of common statutory terms. 785 F.3d at 812; *see id.* at *28 ("we hold that the text of § 215 cannot bear the weight the

government asks us to assign to it, and that it does not authorize the telephone metadata program.").

The same result should obtain here, in which there has been a tangible, improper application of the NSA program.

1. The Information Collected Through NSA's Telephone Metadata Program.

The concept of metadata is a product of the digital revolution, leaving an electronic footprint of the vast array of electronic communications and activities that occur daily in myriad fashion. As the Second Circuit explained in *ACLU v. Clapper*, discussing the NSA's telephone metadata program

> [u]nlike what is gleaned from the more traditional investigative practice of wiretapping, telephone metadata do not include the voice content of telephone conversations. Rather, they include details about telephone calls, including, for example, the length of a call, the phone number from which the call was made, and the phone number called. Metadata can also reveal the user or device making or receiving a call through unique "identity numbers" associated with the equipment (although the government maintains that the information collected does not include information about the identities or names of individuals), and provide information about the routing of a call through the telephone network, which can sometimes (although not always) convey information about a caller's general location.

785 F.3d at 793-94.

In *ACLU v. Clapper*, the Second Circuit also recognized the privacy implications of metadata collection, pointing out "[t]hat telephone metadata do not

directly reveal the content of telephone calls, however, does not vitiate the privacy concerns arising out of the government's bulk collection of such data." Quoting from the briefs from plaintiffs and *amici* therein, the Second Circuit noted "the startling amount of detailed information metadata can reveal – 'information that could traditionally only be obtained by examining the contents of communications' and that is therefore '*often a proxy for content*.'" *Id*. at 794 (emphasis added). *See also id*. at 794, n. 1 (describing study reported in *Science* magazine that "revealed how much information can be gleaned from credit card metadata").

In that context, the Second Circuit elaborated on the distinctions between traditional forms of metadata and that currently available for collection: "the structured format of telephone and other technology-related metadata, and the vast new technological capacity for large-scale and automated review and analysis, distinguish the type of metadata at issue here from more traditional forms." *Id*. at 794.

As a result, "[t]he more metadata the government collects and analyzes, furthermore, the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals." *Id*. Nor is it feasible to escape that intrusion because, as the Court in *ACLU v. Clapper* observed, "in today's technologically based world, it is virtually impossible for an ordinary citizen to avoid creating metadata about himself on a regular basis simply by conducting his

ordinary affairs." *Id*.

2. The Relevant Statute

The initial version of the statute was enacted in 1998 as an amendment to FISA. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub.L. No. 105272, § 602, 112 Stat. 2396, 2410-11 (1998). In 2001, "[t]he PATRIOT Act substantially revised §215 to provide for the production not only of 'business records' but also of 'any tangible things,' and to eliminate the restrictions on the types of businesses such orders can reach." *ACLU v. Clapper*, 785 F.3d at 795 (citing USA PATRIOT ACT of 2001, Pub.L. No. 107–56, §215.)

Prior to 2006, subsection (b)(2) required the Director of the Federal Bureau of Investigation or his designee to "specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

In 2006, Congress reconfigured the section by adding subparagraph (A), and re-designating former subparagraph (A) as subparagraph (B). Thus, the operative

requirement for an application, set forth in §1861(b)(2)(A), became

> a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to–
>
> (i) a foreign power or an agent of a foreign power;
> (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation;
> or
> (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation[.]

50 U.S.C. §1861(b)(2)(A).[20]

3. Disclosure of the Scope of the NSA's Bulk Telephone Metadata Program.

As described in *ACLU v. Clapper*, the NSA program "involves the bulk collection by the government of telephone metadata created by telephone companies in the normal course of their business but now explicitly required by the government to be turned over in bulk on an ongoing basis." 785 F.3d at 793. *See also id.*, at 792 (under the program, NSA "collects in bulk 'on an ongoing daily basis' the metadata associated with telephone calls made by and to Americans, and aggregates those

---

20 The statute was again amended this past June. *See* fn. 27.

metadata into a repository or data bank that can later be queried").

As the opinion in *ACLU v. Clapper* recounted, "Americans first learned about the telephone metadata program that appellants now challenge on June 5, 2013, when the British newspaper *The Guardian* published a FISC order leaked by former government contractor Edward Snowden." 785 F.3d at 793. *See also In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc., ex rel. MCI Commc'n Servs., Inc., d/b/a Verizon Bus. Servs.* ("Verizon Secondary Order"), No. BR 13–80, slip op. at 2 (F.I.S.C. Apr. 25, 2013.) available at: www.fisc.uscourts.gov/sites/default/files/BR%2014-96%20 Opinion-1.pdf.

After that Verizon Secondary Order was published, "the government acknowledged that it was part of a broader program of bulk collection of telephone metadata from other telecommunications providers carried out pursuant to §215." 785 F.3d at 796. In *ACLU v. Clapper*, there was some dispute regarding the scope of the program, as "[t]he government dispute[d plaintiffs'] characterization of the program as collecting 'virtually all telephony metadata' associated with calls made or received in the United States, but decline[d] to elaborate on the scope of the program or specify how the program falls short of that description." 785 F.3d at 797. Yet the Second Circuit responded that "[i]t is unclear, however, in what way [plaintiffs']

characterization of the program can be faulted[,]" *id*., adding that

> if the orders challenged by [plaintiffs] do not require the collection of metadata regarding every telephone call made or received in the United States (a point asserted by [plaintiffs] and at least nominally contested by the government), they appear to come very close to doing so.

785 F.3d at 813.[21]

Accordingly, the Circuit concluded,

> [t]he sheer volume of information sought is staggering; while search warrants and subpoenas for business records may encompass large volumes of paper documents or electronic data, the most expansive of such evidentiary demands are dwarfed by the volume of records obtained pursuant to the orders in question here.

Id.

The government's description of the NSA program was provided by the Court in *ACLU v. Clapper*:

> [t]he government explains that it uses the bulk metadata collected pursuant to these orders by making "queries" using metadata "identifiers" (also referred to as "selectors"), or particular phone numbers that it believes, based on "reasonable articulable suspicion," to be associated with a foreign terrorist organization. Joint App'x 264 (Declaration of Teresa H. Shea). The identifier is used as a "seed" to search across the government's database; the search results yield phone numbers, and the metadata associated with them, that have been in contact with the seed. *Id.* That step is referred to as the first "hop." The NSA can then also search for the numbers, and associated metadata, that

---

21 Here, of course, as set forth ante, at pages 61-65, the U.S. government acknowledged to Congress that it had collected, retained, aggregated, and reviewed Moalin's telephone metadata.

> have been in contact with the numbers resulting from the first search – conducting a second "hop." *Id.* at 265. Until recently, the program allowed for another iteration of the process, such that a third "hop" could be conducted, sweeping in results that include the metadata of, essentially, the contacts of contacts of contacts of the original "seed." *Id.*

785 F.3d at 797.[22]

As a result of the June 2013 disclosure of the categorical scope of the program, several declaratory judgment challenges have been instituted in federal courts nationwide. In addition to *ACLU v. Clapper*, similar lawsuits were commenced in *Smith v. Obama,* 24 F.Supp.3d 1005 (D.Idaho 2014), No. 14-35555 (9th Cir. argued Dec. 8, 2014), and *Klayman v. Obama,* 957 F.Supp.2d 1 (D.D.C.2013), *vacated and remanded*, ___ F.3d ___, 2015 WL 5058403 (D.C. Cir. August 28, 2015).

In *Klayman*, in the context of the NSA program's constitutional flaws, the district court held that the the plaintiffs had demonstrated a likelihood of success on the merits that the NSA program constituted an unreasonable search under the Fourth Amendment. However, last month the D.C. Circuit vacated that ruling and remanded the matter for the district court "to decide whether limited discovery to explore jurisdictional facts is appropriate." 2015 WL 5058403, at *9 (Williams, J.).[23]

---

22 The elimination of that "third hop" is of recent vintage. *See* fn. 27..

23 The question posed by the D.C. Circuit was whether, as Verizon Wireless customers, rather than as Verizon Business Network Services subscribers, the plaintiffs in that declaratory judgment action possessed the requisite standing to

This case, however, presents the only challenge to the NSA program in the context of a criminal prosecution (and represents the only case in which the government has acknowledged that the NSA program played any role in the investigation and/or acquisition of evidence).

4. The NSA Program's Impermissibly Elastic Definition of "Relevance."

In finding that the NSA program had trespassed the boundaries set by Congress in §215, the Second Circuit in *ACLU v. Clapper* focused on the government's limitless, and therefore meaningless – for practical purposes – and ultimately intolerable (for legal purposes) interpretation of "relevance" under the statute.

In reaching its conclusion, the Second Circuit noted that

> "[r]elevance" does not exist in the abstract; something is "relevant" or not in relation to a particular subject. Thus, an item relevant to a grand jury investigation may not be relevant at trial. In keeping with this usage, §215 does not permit an investigative demand for any information relevant to fighting the war on terror, or anything relevant to whatever the government might want to know. It permits demands for documents "relevant to an authorized *investigation.*"

785 F.3d at 815 (emphasis in original).

---

challenge the NSA program. *Klayman*, 2015 WL 5058403, at *5 (Williams, J.). Upon remand, the district court has heard oral argument but not ruled yet. *See* Andrea Noble, "Judge Acknowledges His Own Constitutional Concerns About NSA Phone Snooping," *The Washington Times*, October 8, 2015, available at <http://m.washingtontimes.com/news/2015/oct/8/judge-richard-leon-worries-about-nsa-phone-snoopin/>.

The Court in *Clapper* found that the interpretation the government asked the Court to adopt "defies any limiting principle[,]" 785 F.3d at 818, emphasizing that "the distinction is not merely one of quantity – however vast the quantitative difference – but also of quality." *Id*. at 813 ("[t]he metadata concerning *every* telephone call made or received in the United States using the services of the recipient service provider are demanded, for an indefinite period extending into the future." *Id*. (emphasis in original.))[24]

As a result, the Court decided, "[t]he government's approach essentially reads the 'authorized investigation' language out of the statute." *Id*. at 815-16. Standing firm that "§215's power cannot be interpreted in a way that defies any meaningful limit[,]" the Court in *ACLU v. Clapper* concluded "that to allow the government to collect phone records only because they may become relevant to a possible authorized investigation in the future fails even the permissive 'relevance' test." *Id*., at 818 ("[p]ut another way, we agree with appellants that the government's argument is 'irreconcilable with the statute's plain text'").[25]

---

24 *See also* 785 F.3d at 814 ("[t]he telephone metadata program requires that the phone companies turn over records on an "ongoing daily basis" – with no foreseeable end point, no requirement of relevance to any particular set of facts, and no limitations as to subject matter or individuals covered") (footnote omitted).

25 The same conclusion was reached by the Privacy and Civil Liberties Oversight Board (hereinafter "PCLOB") and Review Group on Intelligence and

Thus, the Court in *Clapper* determined that the statute's "relevance" standard could not justify the staggering scale of collection that occurred under the NSA program.[26]

Communications Technologies (hereinafter "President's Review Group"). *See also* PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, at XX (Jan. 23, 2014) (hereinafter "PCLOB Report"), available at <https:// www.pclob.gov/library/215Report_on_the_Telephone_ Records_Program. pdf>; President's Review Group on Intelligence and Communications Techniques, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Techniques* (Dec. 12, 2013) (hereinafter "PRG Report"), at XX, available at <https://www.whitehouse.gov/sites/default/files/docs/ 201312–12_rg_final_report. pdf>.

The "detailed report" (785 F.3d at 798) issued by PCLOB reached the same conclusion: "that the program was inconsistent with § 215, violated the Electronic Communications Privacy Act, and implicated privacy and First Amendment concerns." *Id*., at 798-99, citing PCLOB Report, at 59-60. According to the PCLOB Report, the NSA program in practice was "little different, in practical terms, from simply declaring that they are relevant to counterterrorism in general . . . At its core, the approach boils down to the proposition that essentially all telephone records are relevant to essentially all international terrorism investigations." *Id.,* at 59–60.

The PCLOB is a an independent, bipartisan agency within the executive branch, established in 2007, the members of which are appointed by the President and confirmed by the Senate, "in order to monitor the actions taken by the government to protect the nation from terrorism and to ensure that they are appropriately balanced against the need to protect privacy and civil liberties." 785 F.3d at 798, citing Implementing Recommendations of the 9/11 Comm'n Act of 2007, Pub. L. No. 110-53, 121 Stat. 266 (2007). *See also* PCLOB Report, at 2.

26 In addition, in *ACLU v. Clapper* the Court determined that "[t]he government's approach also reads out of the statute another important textual limitation on its power under § 215[,]" namely that of the prohibition on collection

5. The NSA Program's Application In This Case

While *ACLU v. Clapper* involved a challenge to the government's collection of telephony metadata, this case is the first to involve a challenge not only to collection of telephony metadata but to the government's use of that data in a criminal investigation and prosecution. Here, the government did not simply collect information about Moalin's communications over an extended period of time – although of course it did that. It also retained those communications, searched them repeatedly, and (eventually) retrieved his records in response to a specific query. It then used the query results to support an application to the FISC, which authorized interception of his telephone calls.

That is precisely the type of collection and use that the Court in *Clapper* found exceeded the authority granted in §215. Referring *to this case*, the Court in *ACLU v.*

---

of records for merely a "threat assessment." *See* §1861(b)(2)(A). 785 F.3d at 816, citing Attorney General's Guidelines for Domestic FBI Operations 16-18 (2008) (hereinafter "AG Guidelines"), available at <https://www.ignet.gov/sites/default/files/files/invprg1211appg1.pdf. *Id.* at 17>. A threat assessment can be conducted on a low threshold, but concurrently with "relatively low intrusiveness, such as obtaining publicly available information, checking government records, and requesting information from members of the public.'" 785 F.3d at 816 (quoting AG Guidelines, at 17-18.) Yet, at the Court in *ACLU v. Clapper* recognized, "[t]he telephone metadata program, however, and the orders sought in furtherance of it, are even more remote from a concrete investigation than the threat assessments that – however important they undoubtedly are in maintaining an alertness to possible threats to national security – Congress found not to warrant the use of §215 orders." 785 F.3d at 817.

Clapper, noted that "[w]hile the government purports to have provided 'examples' of 'specific counter-terrorism investigations,' *see* Appellees' Br. 33, citing Joint App'x 254-55, those examples serve only as instances in which the metadata already collected in bulk were able to be queried and resulted in identification of a previously unknown contact of known terrorists." 785 F.3d at 815 n. 8.

Critically, though, and dispositively here as well, "[t]he government does not contend that most of the metadata already collected were relevant to any of those particular investigations, let alone that it was able to so demonstrate prior to the collection of those metadata." *Id*., at 816. As was the case here, "[o]nly at that point are any of the stored records examined." *Id*.

Moreover, and again pertinent here, "[t]he records sought are not even asserted to be relevant to any ongoing 'systematic examination' of any particular suspect, incident, or group; they are relevant, in the government's view, *because there might at some future point be a need or desire to search them in connection with a hypothetical future*." *Id*. (emphasis added). Consequently, here the ongoing collection and subsequent querying of Moalin's telephone metadata violated §215.

6. Subsequent Developments Reinforce the Conclusion That the NSA Program Collected and Retained Moalin's Metadata In Contravention of §1861.

This past June's significant amendment of the §1861 reinforces the conclusion

that the collection, aggregation, retention, and review of Moalin's telephone metadata violated §1861. In its first comprehensive effort to revamp §1861 since the disclosures by Snowden, Congress this past June enacted the USA FREEDOM Act – Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015. *See* USA Freedom Act of 2015, Public Law No: 114-23 (06/02/2015).

Among other changes, §1861(b)(2)(C) was added to require that, in order to justify "production on an ongoing basis of call detail records,"

> (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and
>
> (ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor[.]

Id.

Thus, the NSA program that existed during the collection, aggregation, retention, and review of Moalin's telephone metadata no longer exists, replaced by the architecture defined in the amended §1861, which by its explicit language and legislative history demonstrates that Congress does not believe that §1861 *ever* authorized bulk telephone metadata collection. *See* H. Rep. No. 114-109, at 18–19

(2015).[27]

7. Appellants Have Standing to Seek Suppression due to the NSA Program's Improper Collection, Retention, Aggregation, and Review of the Telephone Metadata, and Even Dismissal Is an Appropriate Remedy.

Each of the Appellants has the requisite standing to challenge the FISA electronic surveillance – which, in the form of the intercepted telephone conversations, comprised the government's principal evidence at trial – because it was predicated on the fruits of other unlawful surveillance: namely, the NSA's illegal bulk collection, retention, aggregation, and use of Mr. Moalin's telephone metadata.

Under the plain language of FISA,

> [a]ny person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person . . . may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that –
>
> (1) the information was unlawfully acquired; or
>
> (2) the surveillance was not made in conformity with an order of authorization or approval.

---

[27] Also, more recently, in light of the USA FREEDOM Act's limitation on the collection and retention of telephone metadata, the government announced that NSA will, as of November 29, 2015 (the effective date of the Act), no longer be able to search the database holding five years' worth of U.S. domestic telephone calls, and will lose all access to that database (because the information therein will be purged with the exception of that necessary for ongoing litigation). *See* Charlie Savage, "N.S.A. Will Not Be Allowed to Keep Old Phone Records," *The New York Times*, July 27, 2015, available at <www.nytimes.com/2015/07/28/us/politics/nsa-will-not-be-allowed-to-keep-old-phone-records.html>.

50 U.S.C. §1806(e).

It is beyond dispute that Mr. Moalin has standing to challenge both the recording of his telephone calls pursuant to an individualized FISA order, *see* 50 U.S.C. § 1801(k), and the NSA's bulk collection, retention, aggregation, and review of his call records. *See Clapper*, 785 F.3d at 801-02.

Appellants Mohamud, Doreh, and Nasir also have "standing" to seek suppression under section 1806(e). There is no question that appellants Mohamud, Doreh, and Nasir are "aggrieved persons" under section 1806(e), as their conversations were intercepted pursuant to the FISA warrant, and an "aggrieved person" means "any person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Accordingly, they are permitted to make a claim that such information "was unlawfully acquired . . . ." 50 U.S.C. § 1806(e).

The use of the "information was unlawfully acquired" language in section 1806(e) is different and more broad than the language used in Title III, and it is presumed that Congress acted intentionally when it incorporated the different language. *See Custis v. United States*, 511 U.S. 485, 492 (1994); *see also Dean v. United States*, 556 U.S. 568, 573 (2009) (quoting *Russello v. United States*, 464 U.S. 16, 23 (1983)). Under Title III, an "aggrieved person" may move to suppress the

contents of an intercepted communication "on the grounds that – (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval." 18 U.S.C. § 2518(10)(a). Thus, an aggrieved person may only move to suppress under Title III if a particular "communication" was "unlawfully intercepted," whereas an aggrieved person may move to suppress under FISA if "information" was "unlawfully acquired." As argued earlier in this brief, and as confirmed in *Clapper*, all of the information obtained pursuant to the FISA warrant had an unlawful genesis and therefore was "unlawfully acquired."

Furthermore, like Moalin, all of the appellants were subjected to the unlawful telephone metadata program. As explained in *Clapper*, their metadata information, like the information of tens of millions of others, was "seized" pursuant to the unlawful program. They therefore have "standing" to assert the program's illegality as a basis for a motion to suppress. *Cf. Clapper*, 785 F.3d at 801-02 (the mere collection of the metadata constitutes a "seizure" that bestowed standing, even if that metadata was not specifically "searched").[28] In this sense, this case is significantly

[28] The metadata of Mohamud, Doreh, and Nasir could have been swept up in a first, second, or third "hop" from Moalin's metadata. *See Clapper*, 785 F.3d at 797.

different from *United States v. Payner*, 447 U.S. 727 (1980), where the Supreme Court held that a district court improperly suppressed evidence pursuant to its supervisory powers even though the defendant's constitutional rights were not violated. Here, all of the appellants' rights were violated by the metadata program, and there is a specific statutory scheme authorizing the exclusionary rule as a remedy for the unlawful acquisition of information by the government.[29]

Finally, putting aside the exclusionary rule, dismissal of the indictment as to all Appellants is required to implement a remedy for the government's widespread collection of personal information without statutory authorization and the resulting Fourth and Fifth Amendment implications, particularly given the posture of this case. A court may dismiss an indictment with prejudice for outrageous government conduct amounting to a due process violation, or pursuant to its supervisory powers "to implement a remedy for the violation of a recognized statutory or constitutional right; to preserve judicial integrity by ensuring that a conviction rests on appropriate considerations validly before a jury; and to deter future illegal conduct." *United*

---

[29] While the statutory scheme specifically calls for suppression, it should also be noted that this Court has repeatedly suppressed evidence obtained in violation of a statute or procedural rule that is tied to constitutional interests. *See, e.g.*, *United States v. Soto-Soto*, 598 F.2d 545, 548 (9th Cir. 1979) (suppressing evidence obtained during border search that violated 19 U.S.C. § 482); *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992) (suppressing evidence obtained in violation of Rule 41, Fed.R.Crim.P.).

States v. Chapman, 524 F.3d 1073, 1084-85 (9th Cir. 2008). In this case, the failure to disclose the role of the unlawful metadata program in this prosecution in a timely and voluntary manner amounted to a due process violation, and, at the very least, constitutes sufficient grounds for dismissal under the Court's supervisory powers. *See Chapman*, 524 F.3d at 1085-88 (dismissal of indictment pursuant to supervisory powers for *Brady* violation). Dismissal is an appropriate remedy even if the prosecutors were unaware of the role of the unlawful metadata program in the initiation of this prosecution. *See United States v. Blanco*, 392 F.3d 382, 393-95 (9th Cir. 2004).

II.

THE NSA PROGRAM'S COLLECTION, AGGREGATION, RETENTION, AND REVIEW OF MOALIN'S TELEPHONE METADATA VIOLATED THE FOURTH AMENDMENT.

The NSA program's collection, aggregation, retention, and review of Moalin's telephone metadata separately and collectively violated the Fourth Amendment's proscription against warrantless and/or unreasonable searches and seizures.

However, determination of that constitutional issue is not necessary to resolve this appeal in defendants' favor. Indeed, decision on the statutory bases set forth in the first argument is favored by the canons of judicial review, which dictate "constitutional avoidance," the doctrine that "allows courts to *avoid* the decision of

constitutional questions" by providing "a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." *Clark v. Martinez,* 543 U.S. 371, 381 (2005) (emphasis in original).

That was the course of the Second Circuit in *ACLU v. Clapper* addressing the statutory issue and avoiding the constitutional questions (which it noted "present[] potentially vexing issues"). *Id*. at 821 (footnote omitted); *see also id*., at 808-09 (discussing why constitutional avoidance encouraged judicial review of the NSA's telephone metadata program); *id*., at 810 (regarding plaintiffs' statutory challenge, court "naturally turn[s] first that argument").

As the Second Circuit recognized, properly understood, Section 215 is not a departure from the longstanding constitutional tradition prohibiting arbitrary searches – it is a reflection of it.

The government collected Moalin's call records on a daily basis and aggregated them with the call records of millions of other Americans. The call records so collected indicated whom Moalin had called, and when, and for how long. By aggregating Moalin's records with those of other Americans, the government created a massive and ever-growing database that displayed not just Moalin's direct associations, but also his *in*direct associations – not just whom Moalin had called, but

also whom *those persons* had called, and who *those* people had called, and so on. Indeed, as FBI Deputy Director Joyce testified before Congress, Molain's contact with an alleged "extremist" overseas was "indirect." (CR 345-2.)

The collection of Moalin's call records was itself a substantial intrusion on his constitutionally protected privacy, but the government did not merely collect those records. It aggregated, retained, and reviewed them as well, subjecting the database to searches on hundreds of occasions. On at least one such occasion, the query returned Moalin's telephone number, indicating that Moalin had been in contact – again, only *in*directly, according to government officials – with a person connected to terrorism.

The government's entire investigation of Moalin was predicated on that information, which was obtained, retained, and utilized by means of a series of unconstitutional searches and/or seizures. As the analysis below establishes, at each successive stage – collection, aggregation, retention, and review – the government conducted an unlawful search and/or seizure that violated the Fourth Amendment.

In assessing whether the NSA program violated the Fourth Amendment's proscription on warrantless and/or unreasonable searches and seizures, two primary issues require analysis:

- did the NSA program's collection, aggregation, retention,

and review of Moalin's telephone metadata constitute a search or seizure for Fourth Amendment purposes?

- was the NSA program's long-term collection, aggregation, retention, and review of Moalin's telephone metadata unreasonable?

As set forth, the inescapable conclusion resulting from that analysis is that the NSA program, in collecting, aggregating, retaining, and reviewing Moalin's telephone metadata, conducted an unreasonable search and seizure that violated the Fourth Amendment.

A. Moalin Possessed a Reasonable Expectation of Privacy In His Telephone Metadata With Respect to the NSA's Program.

Moalin possessed a reasonable expectation of privacy with respect to his telephone metadata, particularly in the context of the NSA program's scope in terms of the breadth of its collection and aggregation, its retention, and the nature of its review. Moreover, contrary to the district court's decision, *Smith v. Maryland*, does *not* control that question here.

Applying the familiar test described by Justice Harlan in *Katz v. United States*, 389 U.S. 347 (1967) – that is, by asking whether individuals have a reasonable expectation of privacy in the information the government seeks – the answer is clear. *Id*., at 360–61 (Harlan, J., concurring).

ACLU v. Clapper recognized the sensitivity of telephone metadata, particularly

when collected over extended periods, aggregated in a database, and searched at a later date. *See also* PCLOB Report, 156-57; PRG Report 110-14, 116-17.

In addition, the duration of the collection, and the amount of information acquired, is also a factor in establishing a reasonable expectation of privacy. Those considerations led a majority of the Supreme Court in *United States v. Jones*, ___ U.S. ___, 132 S. Ct. 945 (2012), to recognize that the long-term collection of personal data concerning even one individual can intrude upon a reasonable expectation of privacy when more limited surveillance might not. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring).

As the Second Circuit explained in *Clapper*, "[t]he more metadata the government collects and analyzes, . . . the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals." *Clapper*, 785 F.3d at 794; *see also Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (noting that long-term location tracking "enables the government to ascertain, more or less at will, [every person's] political and religious beliefs, sexual habits, and so on").[30]

---

30 The pervasiveness of the NSA program evokes the following passage from George Orwell's *1984*:

> [h]ow often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate, they could plug in your wire whenever they wanted to. You had to live – did live, from habit that

What the Supreme Court observed of long-term monitoring in *Jones* is equally true of the bulk collection of Americans' telephone records in general, and Moalin's here. *See Clapper*, 785 F.3d at 823; PCLOB Report 156-58. These features of the call-records program – features the government has never disputed – compel the conclusion that the government intruded upon a reasonable expectation of privacy when it collected, aggregated, retained, and reviewed Moalin's telephone metadata. *See United States v. Nerber*, 222 F.3d 597, 599 (9th Cir. 2000) (Fourth Amendment requires person have "expectation that his activities would be private").

That Moalin's expectation of privacy in his aggregated and retained metadata is recognized by society as reasonable is reinforced by the fact that, "in today's technologically based word, it is virtually impossible for an ordinary citizen to avoid creating metadata about himself on a regular basis simply by conducting his ordinary affairs[.]" *Clapper*, 785 F.3d at 794; *see Klayman*, 957 F. Supp. 2d at 35-36 ("the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the government about people's lives. . . . I think it is . . . likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as

---

> became instinct – in the assumption that every sound you made was overheard, and, except in darkness every movement scrutinized.

George Orwell, *1984*, at 3 (Signet Classics 1950).

reasonable") (emphasis in original); *see also City of Ontario v. Quon*, 560 U.S. 746, 760 (2010) ("[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy").[31]

The aggregation from a trove of electronically stored information available on digital devices also influenced the Court's decision in *Riley*:

> [t]he storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions;

[31] Indeed, the reasonableness of an expectation of privacy in metadata becomes even more plain when one considers the consequences of the contrary result. As one judge has explained: "[i]f a telephone caller does not want to reveal dialed numbers to the telephone company, he has another option: don't place a call. If a cell phone user does not want to reveal his location to a cellular carrier, he also has another option: turn off the cell phone." *United States v. Davis*, 785 F.3d 498, 519 (11th Cir. 2015) (Pryor, J. concurring). The patent unreasonableness of these so-called "options" in today's digitally connected world underscores the objective reasonableness with which society would regard Moalin's expectation of privacy in this case. *See Clapper*, 785 F.3d at 824 ("individuals can barely function without involuntarily creating metadata that can reveal a great deal of information about them"). *See also Riley*, 134 S. Ct. at 2485 ("[t]hese cases require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy").

> the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier.

Id., at 2489.[32]

Similarly, even more recently, in *United States v. Graham*, 796 F.3d 332 (4th Cir. 2015), the Fourth Circuit, in rejecting the government's argument that because a third party had possession (and even ownership) of the defendant's cell site location information ("CSLI"), that defendant lacked a reasonable expectation of privacy, explained that

> [e]xamination of a person's historical CSLI (cell site location information) can enable the government to trace the movements of the cellphone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. *Cellphone users have an objectively reasonable expectation of privacy in this information*. Its inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies.

Id., at 345 (emphasis added).[33]

---

[32] *See also What's Old Is New Again: Retaining Fourth Amendment Protections In Warranted Digital Searches (Pre-Search Instructions and Post-Search Reasonableness)* A Report by the National Association of Criminal Defense Lawyers' Fourth Amendment Advocacy Committee, May 18, 2014 (hereinafter "*NACDL Report*"), available at <http://www.nacdl.org/NewsReleases.aspx?id=33866>, at 1 ("[w]hat is different is the amount of private information that can be improperly searched and the substantially greater intrusion upon privacy and Fourth Amendment interests that may result").

[33] In *Graham*, the Court nevertheless declined to suppress because the law enforcement agents had relied in good faith on orders (rather than warrants) issued

As the Court in *Graham* declared, "[w]e cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person." *Id*. at 356.[34]

Thus the district court herein – which did not have the benefit of *Riley*, or *ACLU v. Clapper*, or *Klayman*, or *Graham*, all of which were decided subsequently – was incorrect in failing to recognize Moalin's *objective* expectation of privacy. (CR 386 at 12: while Moalin "may have had some degree of a subjective expectation of privacy" in the call records the government had collected, his Fourth Amendment claim would fail the *Katz* test because, under *Smith*, his "expectation is not 'one that society is prepared to recognize as reasonable'", quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

The district court also erred in relying on *Smith v. Maryland,* 442 U.S. 735 (1979). Given the vast differences between the facts of the targeted criminal investigation in *Smith* and the NSA call-records program that ensnared Moalin's records, *Smith* cannot bear the weight the district court placed on it.

---

pursuant to the Stored Communications Act (28 U.S.C. §2703).

[34] Concurring in *Graham*, Judge Thacker wrote "to express [his] concern about the erosion of privacy in this era of rapid technological development." Graham 796 F.3d at 377 (Thacker, J., concurring).

In *Smith*, the Supreme Court held that a telephone subscriber does not have an expectation of privacy in the numbers he or she dials because the subscriber knows that the telephone company keeps records of that information (which the subscriber has at least tacitly "knowingly" provided to that third party). Yet the facts of *Smith*, and the intrusion it endorsed, are dramatically different from the NSA program's long-term and dragnet collection, aggregation, retention, and subsequent review of Moalin's call records.

In *Smith*, Baltimore police suspected that Michael Smith was making threatening and obscene phone calls to a woman he had robbed days earlier. To confirm their suspicions, they asked Smith's telephone company to install a "pen register" on his phone line to record the numbers he dialed. 442 U.S. at 737. After just three days, the pen register confirmed that Smith was the caller. *Id.*

Also, the Court in *Smith* noted in support of its reasoning that the pen register did "not indicate whether calls are actually completed." *Id*., at 736 n. 1, quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 161 n. 1 (1977). *See also id*., at 741 ("a law enforcement official could not even determine from a pen register whether a communication existed"). Again as part of its justification, the Court added that "[n]either the purport of any communication between the caller and recipient of the call, their identities, nor whether the call was even completed is disclosed by pen

registers." 442 U.S. at 741, quoting *United States v. New York Tel. Co.*, 434 U.S. at 167.

The Court in *Smith* further based its decision on the fact that pen registers were "routinely used by telephone companies 'for the purpose of checking billing operations, detecting fraud, and preventing violations of law.'" 442 U.S. at 742, quoting *New York Tel. Co.*, at 174-75. *See also id*. (also "to check for a defective dial, or to check for overbilling") (citation omitted) (internal quotation marks omitted).

Here, the NSA program was exponentially more invasive of privacy than the primitive, short-term pen register at issue in *Smith*. The surveillance in *Smith* occurred for three days, but the surveillance at issue here was effectively permanent. The surveillance in *Smith* was elementary and narrow, involving only the numbers dialed, but the surveillance at issue here is much broader, encompassing (among other things) the duration of calls. The call records in *Smith* were collected for immediate review in connection with a specific investigation of a crime already committed, but the call records at issue here were collected "only because they may become relevant to a possible authorized investigation in the future." *Clapper*, 785 F.3d at 818.

Moreover, the surveillance in *Smith* was directed at a single criminal suspect on the basis of individualized suspicion, but the surveillance at issue here collected Moalin's call records along with those of hundreds of millions of people absent any

individualized justification, and then combined them to create a searchable database, thereby magnifying the injury to Moalin.

The aggregation of records compounded the invasiveness and impact of the NSA program upon Moalin's privacy because the government acquires more information about any given individual by monitoring the call records of that individual's contacts – and by monitoring the call records of those *contacts'* contacts. *See United States v. Nerber*, 222 F.3d 597, 600 (9th Cir. 2000) ("[w]e reject the government's broad argument that a court may never consider the severity of the governmental intrusion in determining whether a citizen has a legitimate expectation of privacy"). *See also Clapper*, 785 F.3d at 822-23 ("rules that permit the government to obtain records and other information that consumers have shared with businesses without a warrant seem much more threatening as the extent of such information grows"); *Klayman v. Obama*, 957 F. Supp. 2d 1, 31 (D.D.C. 2013), *vacated and remanded on other grounds*, ---- F.3d ---- (D.C. Cir. ------ 2015). *See also Riley*, 134 S. Ct. at 2489.

While the district court cited post-*Smith* decisions, including decisions of this Court, that applied *Smith* to other contexts, (CR 388 at 10-11,) those cases, much like *Smith* itself, involved only individualized collection of customer records based on individualized suspicion of criminal activity. *See United States v. Reed*, 575 F.3d 900,

906, 914 (9th Cir. 2009); *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1111, 1116 (9th Cir. 2012).

As a result, it would be particularly inappropriate to hold that *Smith* – again, a case involving a very short-term and particularized, individualized surveillance of a person suspected of already having committed the specific crime under investigation – permitted the warrantless surveillance – including not only collection, but aggregation, retention, and review – of Moalin's telephone metadata when the Supreme Court has expressly recognized that long-term dragnet surveillance raises distinct constitutional concerns.

Indeed, the Court made this explicit just four years after it decided *Smith*, when it considered the government's warrantless use of a beeper to track the car of a suspected manufacturer of narcotics. *See United States v. Knotts*, 460 U.S. 276 (1983). While in *Knotts* the Court found the defendant lacked a reasonable expectation of privacy in his public movements in the circumstances of that case, it cautioned that *Smith* could not be read to justify "twenty-four hour surveillance of any citizen of this country." *Id.* at 283 (quotation marks omitted). "Dragnet type law enforcement practices," the Court wrote, would present a different constitutional question. *Id.* at 284; *see also United States v. Pineda-Moreno*, 591 F.3d 1212, 1216 n.2 (9th Cir. 2010) (reserving constitutional questions concerning "programs of mass

surveillance") (quotation marks and citation omitted)), *vacated in light of recent decision*, 132 S. Ct. 1533 (2012).

The D.C. Circuit addressed that distinct constitutional question in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012), holding that the government's 28-day tracking of an individual's movements amounted to a Fourth Amendment search. *See Clapper*, 785 F.3d at 823 (noting that the "opportunity" for the Supreme Court to consider the distinct constitutional question raised by dragnet surveillance "came decades later, in *Jones*").

The D.C. Circuit rejected the government's invitation to read *Knotts* – a case that, like every single case cited by the district court and the government in this case, involved targeted surveillance – to authorize long-term warrantless monitoring. *Knotts* did not hold, the D.C. Circuit wrote in *Maynard*, that an individual "has no reasonable expectation of privacy in his movements whatsoever, world without end, as the government would have it." 615 F.3d at 557.

Unanimously affirming *Maynard* in *Jones*, all nine justices of the Supreme Court agreed with the D.C. Circuit's conclusion that long-term surveillance raises distinct and novel questions not controlled by prior precedent. The Supreme Court ultimately decided *Jones* on trespass grounds, not on the basis of the expectation-of-

privacy analysis relied on by the D.C. Circuit in *Maynard*. But the Court's plurality opinion in *Jones* acknowledged that "it may be that achieving [long-term tracking] through electronic means, without an accompanying trespass [as had occurred in *Jones*], is an unconstitutional invasion of privacy," leaving the question for another day. *Jones*, 132 S. Ct. at 954.

In *Jones*, the Court traced the evolution of Fourth Amendment jurisprudence, from an exclusively property law-oriented analysis based on concepts of trespass, embodied in *Olmstead v. United States*, 277 U.S. 438 (1928), and continued through *Silverman v. United States*, 365 U.S. 404 (1961), to evaluation of a person's reasonable expectation of privacy, first enunciated formally in *Katz v. United States*, 389 U.S. 347 (1967). 132 S. Ct. at U.S. ___, 132 S. Ct. 945, 949-50; *see also Kyllo v. United States*, 533 U.S. 27, 32 (2001) (Court has "since decoupled violation of a person's Fourth Amendment rights from the trespassory violation of his property"), citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).[35] Thus, while *Jones* was decided

[35] In *United States v. Davis*, 754 F.3d 1205, 1211 (11th Cir. 2014), *reversed on other grounds*, 785 F.3d 498, 519 (11th Cir. 2015) , the Court recounted that there exist "two distinct views of the interests protected by the Fourth Amendment's prohibition of unreasonable searches and seizures. The older of the two theories is the view that the Fourth Amendment protects the property rights of the people." *Id*. at 1212. However, as the Court added, "in the twentieth century, a second view gradually developed: that is, that the Fourth Amendment guarantee protects the privacy rights of the people without respect to whether the alleged 'search' constituted a trespass against property rights." *Id*. at *4; *see also id*., at 4-5 (tracing the evolution of the privacy theory).

technically on a property-oriented basis, the Court added that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." 132 S. Ct. at 953 (emphasis in original).

In addition, the concurring opinions in *Jones* provided an alternate rationale for the result: that regardless whether there had been a trespass, the *Katz* "expectation of privacy" dictated application of the Fourth Amendment's protection in the context of 28-day long GPS monitoring of the defendant's movements. 132 S. Ct. at 954-57 (Sotomayor, J., concurring) ("at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'"), quoting *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *id*. at 957-64 (Alito, J., concurring) ("lengthy monitoring that occurred" in *Jones* would not have survived the *Katz* test). *See also Clapper*, 785 F.3d at 823-24.[36]

More explicitly, Justice Sotomayor, in concurring in *Jones*, challenged the continued vitality of the third-party records doctrine underlying *Smith*:

> [m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *See, e.g., Smith* [*v. Maryland*], 442 U.S. [735], 742 [(1979)]; *United States v. Miller,* 425 U.S. 435, 443

[36] Justice Alito's concurrence in *Jones* was joined by Justices Ginsburg, Breyer, and Kagan. Thus, including Justice Sotomayor, who concurred separately, the number of Justices who would have grounded the result in an expectation of privacy outnumbered those who relied on the property law basis and refrained from reaching the *Katz*-based rationale.

> (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post,* at 962, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

Two years later, in *Riley v. California*, the full Court addressed a related point in the context of cell phones, noting "there is an element of pervasiveness that characterizes cell phones but not physical records. . . . Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different." 134 S. Ct. at 2490, citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *id.* at 2489.

The Court's elaboration focused on smartphone technologies, but its observation applies equally to call records, in which context new technology "allows

even just one type of information to convey far more than previously possible." *Id.* at 2489. Notably, the Court in *Riley* specifically observed that thousands of photos could reconstruct the "sum of an individual's private life" in a way that just one or two photos could not. *Id.* While *Riley*'s factual context involved a search incident to arrest, the more profound relevance of the Court's decision, especially to this case, is the Court's acknowledgment of the need for the Fourth Amendment to recognize and adapt to the technological advancement accompanying the digitization of communication, storage, and surveillance.

Thus, while in 1928 Chief Justice Taft could, in *Olmstead*, write that the Fourth Amendment could not be "extended and expanded to include telephone wires reaching to the whole world[,]" at 465, by 1967 *Katz* would reject that limitation in favor of an analytical approach that would harmonize Fourth Amendment values with burgeoning technological mores. It is now another 36 years from the decision in *Smith v. Maryland*, 442 U.S. 735 (1979), and 39 years since *United States v. Miller*, 425 U.S. 435 (1976) (also cited by the district court, CR 388 at 10; ER 79), was decided, and again during that interval technology has compelled re-evaluation of just what the Fourth Amendment protects.[37]

[37] Thus has it been since enactment of the Fourth Amendment. It was not until the Pony Express, which began its service in 1860, became popular that the issue of mail privacy – personal papers existing outside the home – merited the Supreme Court's attention. *Ex Parte Jackson*, 96 U.S. 727,733 (1877) (holding that "[t]he

Many justices – often in dissent or concurrence – have been prescient with respect to the necessity for the Fourth Amendment to acknowledge the impact of technology on the concepts of privacy, surveillance, and government intrusion. For example, in his dissent in *Goldman v. United States*, 316 U.S. 125 (1942), Justice Murphy observed that "science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forbears." 316 U.S. at 139 (Murphy, J., dissenting); *see also Olmstead,* 277 U.S. at 474 (Brandeis, J., *dissenting*) ("[w]ays may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the house"); *Lopez v. United States*, 373 U.S. 427, 441 (1963) (Warren, C.J., concurring) (warning that "the fantastic advances in the field of electronic communications constitute a great danger to the privacy of the individual," and that "indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments"); *Dow Chemical Co. v. U.S.*, 476 U.S. 227, 251 (1986) (Powell, J., concurring in part and dissenting in part) (observing that "privacy rights [c]ould be seriously at risk as

constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be[,]" such as "in the mail"); *see also United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

technological advances become generally disseminated and available in our society"); *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (Posner, J.) ("[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive"); *Alliance to End Repression v. City of Chicago*, 627 F.Supp. 1044, 1054 (N.D. Ill. 1985) ("[i]t seems that there should come a point when, in tenaciously tracking and piecing together the details of a person's life from multifarious sources, the resulting probe becomes so intrusive as to amount to an invasion of privacy even if the individual pieces of the probe are from public sources"); *Nader v. General Motors Corp*., 25 N.Y.2d 560, 572 (N.Y. 1970) (Breitel, J., concurring) ("[a]lthough acts performed in 'public,' especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous").

The future envisioned in those opinions has in many respects been realized. *See People v. Weaver*, 12 N.Y.3d 433, 442 (N.Y. Ct. App. 2009) (noting that *Knotts* reserved the question of "twenty-four hour surveillance of any citizen" for another day, and observing that "[t]o say that that day has arrived involves no melodrama; 26 years after *Knotts*, GPS technology, even in its present state of evolution, quite simply

forces the issue").

In that context, the Supreme Court has long recognized the need to apply the Fourth Amendment in a manner that maintains its purposes despite changes in the technological or other circumstances in which Fourth Amendment issues are presented.

For instance, in *United States v. Chadwick*, 433 U.S. 1 (1977), Justice Burger noted that while the Framers "focused on the wrongs of that day," they also "intended the Fourth Amendment to safeguard fundamental values which would far outlast the specific abuses which gave it birth." *Id*. at 9. *See also Goldman*, 139 U.S. at 138 (Murphy, J., dissenting) (Court assumes a "duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation"); Andrew E. Taslitz, *Reconstructing The Fourth Amendment: A History of Search and Seizure*, 1789–1868 51 (2006) ("[t]he Framers' history ultimately matters most when revealing the *values* that originally animated adoption of the amendment . . . [to] allow us to refocus attention on the critical question of what a 'right to be secure' *should* mean").[38]

[38] The Second Circuit, too, has articulated the courts' obligation to resolve these issues in a contemporary context. In *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014), *rehearing en banc granted* 2015 U.S. App. LEXIS 11143 (2d Cir., June 29, 2015), the Circuit remarked that "[a]pplying 18th Century notions searches and seizures to modern technology, however, is easier said than done, as we are asked to measure Government actions taken in the 'computer age' against Fourth Amendment

In light of those principles, and the prospect of untrammeled government access to electronically stored information simply because it is technically in the possession of a third party, a commentator remarks that "this state of affairs poses one of the most significant threats to privacy in the twenty-first century." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1087 (July 2002).

Here, the context includes not only all of Moalin's telephone call records for an extended period, but also the ability to store and search that information indefinitely – and to aggregate it for purposes of searching the telephone metadata of others, too, over that same unlimited span. In both *Jones* and *Riley*, the Court established a Fourth Amendment jurisprudence sensitive to the evolving status of electronically stored information, and its functionality for law enforcement as a tool for pervasive automated surveillance. *See Riley*, 134 S. Ct. at 2484 ("[b]ut while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones").

---

frameworks crafted long before this technology existed." *Id*. at *6 (footnote omitted). The Court in *Ganias* also recognized that "[b]ecause the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools." *Id.* at *19.

Conducting a balancing test – "assessing, on the one hand, the degree to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests[,]" *id*. quoting *Wyoming v. Houghton,* 526 U.S. 295, 300 (1999) – frozen in a previous time, the Court realized, would not be consistent with Fourth Amendment values and protections. *See also id*. at 2496-97 (Alito, J., concurring) ("we should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form. This calls for a new balancing of law enforcement and privacy interests").[39]

Consequently, while conceding that "a mechanical application of *Robinson* might well support the warrantless searches at issue here[,]" the Court nonetheless concluded that justifying a cell phone search based on "pre-digital analogues" would result in 'a significant diminution of privacy[,]'" *id*. at 2493, and held that ". . . officers must generally secure a warrant before conducting such a search." *Id*. at 2485.

---

39 *See also NACDL Report*, at 3 ("in light of today's digital realities[] . . . Courts are attempting to balance the competing needs for both citizens' privacy and effective law enforcement").

Riley thus confirms the obvious: analog-era precedents cannot be extended mechanically to factual contexts dramatically different from those that gave rise to them. Instead, new applications of old precedents to substantially more intrusive contexts "must rest on [their] own bottom[s]." 134 S. Ct. at 2489.

Consequently, the Supreme Court in *Riley* unanimously rejected the government's "strained" attempt to analogize cell-phone searches to the searches of physical items, like packs of cigarettes, that the Court had approved decades earlier in *Robinson*. *See id.* at 2491; *id.* at 2489 ("[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together"); *id.* at 2484–89 [discussing *Chimel* and *Robinson* (1973)].

Moreover, the need to act now, rather than waiting, to modernize Fourth Amendment law, was not lost on the Court in *Riley*: "[w]e expect that the gulf between physical practicability and digital capacity will only continue to widen in the future." *Id*. at 2489. The pace of technological advancement has accelerated obsolescence with respect to products themselves, and threatens to do so legally if courts are not responsive.

As this Court has recognized, in assessing the intrusiveness and ultimately the reasonableness of government action, "technology matters." *United States v.*

Cotterman, 709 F.3d 952, 965 (9th Cir. 2013) (Supreme Court case authorizing a suspicionless border search of a car did *not* authorize a suspicionless comprehensive search of the digital contents of an electronic device).

Thus, this Court has recognized that the mere fact that a person entrusts digital information to a third party is not automatically accompanied by a concurrent surrender of the constitutional right to privacy in that information. For example, a person sending an email "voluntarily discloses" the electronic contents of the email to the email provider so that the email may be transmitted. Yet the email sender nonetheless retains a reasonable expectation of privacy in the email. *See Cotterman*, 709 F.3d at 964 (recognizing that emails "are expected to be kept private and this expectation is 'one that society is prepared to recognize as reasonable'"), quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring); *see also United States v. Warshak*, 631 F.3d 266, 286-87 (6th Cir. 2010).

In a trajectory that arcs at least as far back as *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) and the Pony Express (fn. 36), changes in technology, transportation, and communication have required the courts to navigate a path for the Fourth Amendment that adheres to its fundamental purpose, and applies its fundamental protections.

Thus, *Smith* no more controls the outcome in this case than *Knotts* controlled the outcome in *Maynard* or the reasoning of the concurrences in *Jones*. Likewise,

Smith no more controls in this case than *Chimel* and *Robinson* did in *Riley*. Judge Leon, in *Klayman*, appropriately applied this logic to the question of *Smith*'s relevance to the call-records program: "the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones." 957 F. Supp. 2d at 37, *vacated and remanded on other grounds*, ___ F.3d ___, 2015 WL 5058403 (D.C. Cir. August 28, 2015).

Here, the district court, before *Riley*, *ACLU v. Clapper*, *Klayman*, or *Graham*, failed to appreciate these distinctions, concluding instead that "pen register-like devices predate the internet era by about 150 years and are not a product of the so-called digital revolution." (CR 386 at 12.) Yet, as the Court in *Clapper* acknowledged,

> [m]etadata today, as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis with respect to all of an individual's calls (and not merely, as in traditional criminal investigations, for a limited period connected to the investigation of a particular crime), permit something akin to the 24-hour surveillance that worried some of the Court in *Jones*. Moreover, the bulk collection of data as to essentially the entire population of the United States, something inconceivable before the advent of high-speed computers, permits the development of a government database with a potential for invasions of privacy unimaginable in the past.

785 F.3d at 824.

The surveillance in *Smith* and the surveillance in this case differ in quantity, quality, and functionality, and those vast and material differences demonstrate that the NSA program constituted a novel and unprecedented, but nevertheless indisputable, intrusion upon Moalin's reasonable expectation of privacy.

B. The NSA Program's Collection, Aggregation, Retention, and Review of Moalin's Telephone Metadata Constituted a Search.

A "search" under the Fourth Amendment occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. at 33; *see Katz v. United States*, 389 U.S. at 361 (Harlan, J., concurring). Moreover, "a violation of the [Fourth] Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion." *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990), quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974); *accord ACLU v. Clapper*, 785 F.3d at 801.

As set forth above, in part II.A, the government's ongoing collection, aggregation, retention, and review of Moalin's call records invaded a reasonable expectation of privacy. As a result, the government searched Moalin within the meaning of the Fourth Amendment. In fact, it searched him multiple times in multiple ways, through the collection of his call records and then again through the

aggregation of his call records. The government has argued that the collection and aggregation of call records does not constitute a search. That is not so, but even if it were, the government's eventual review of Moalin's telephone metadata in 2007 (via the query methodology) unquestionably constituted a classic, unadorned search. Indeed, in defending the NSA program against civil lawsuits, the government has conceded that the querying and review of an individual's call records—as occurred with Moalin's telephone metadata—would constitute a search for Fourth Amendment purposes. *See* Gov't Reply in Support of Mot. to Dismiss, at 3 n.6, *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), ECF Dkt. No. 69 (acknowledging "the critical distinction [] between obtaining records and examining them"), *rev'd* 785 F.3d 787 (2d Cir. 2015).

The government has also contended that "the absence of . . . human review" of telephone metadata collected under the NSA program "mean[s] that no infringement of a Fourth Amendment privacy interest demonstrably occurred" in the civil challenges to the program. Brief for Appellees at 36, *Smith v. Obama*, No. 14-35555 (9th Cir. Oct. 2, 2014), ECF Dkt. No. 55-1; *see id.* ("[w]here telephony metadata associated with a particular call remains unreviewed and never comes to any human being's attention, there is no invasion of any constitutionally cognizable privacy

interests . . . .") (emphasis added).[40] And it has argued that the NSA program's invasion of Americans' privacy is minimized because most of the collected data is never reviewed by a human being. *Id*. at 65. Here, of course, Moalin's metadata *was reviewed by a human being* as the result of a deliberate query of the call-records database conducted after its collection and aggregation.

Accordingly, even if the government were correct (which it is not) that the collection and aggregation of Moalin's call records did not constitute a search under the Fourth Amendment, the government's retention and review of Moalin's telephone metadata unquestionably did.

C. The NSA Program's Collection, Aggregation, Retention, and Review of Moalin's Telephone Metadata Constituted a Seizure.

For similar reasons, the collection of Moalin's call records is also a "seizure" for Fourth Amendment purposes. As the Second Circuit pointed out in *ACLU v. Clapper*, "[t]he Fourth Amendment protects against unreasonable searches *and*

---

40 Notwithstanding the government's contention, this Court has recognized that such a distinction is of no moment for Fourth Amendment purposes. *See Cotterman*, 709 F.3d at 958 (treating government's use of "forensic software that often must run for several hours to examine" files stored on hard drives as a Fourth Amendment "search"). *See also United States v. Crist*, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008) (government's use of "hash" analysis to review all computer files a Fourth Amendment "search" regardless of fact that no human agents looked at any files); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 568 (D. Md. 2014) (similar).

seizures." 785 F.3d at 801 (emphasis in original).Just as in *Clapper*, here Moalin's "records (among those of numerous others) have been targeted for seizure by the government . . . and the records have been collected." *Id.* at 801-02; *see United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171-72 (9th Cir. 2010) (en banc) (*per curiam*) (characterizing government's copying of electronic data as a seizure); *Katz*, 389 U.S. at 354 (categorizing government's recording of phone call as a "search and seizure"); *United States v. Ganias*, 755 F.3d at 137,*rehearing en banc granted* 2015 U.S. App. LEXIS 11143 (2d Cir., June 29, 2015) (government's denying defendant "exclusive control over" copies of digital files constituted a "meaningful interference with . . . possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment").

In fact, in *ACLU v. Clapper*, the Court expressed its view that "such collection is more appropriately challenged, at least from a standing perspective, as a seizure rather than as a search." 785 F.3d at 801; *see also United States v. Verdugo-Urquidez,* 494 U.S. at 264 (internal quotation marks omitted.)

The retention of Moalin's telephone metadata for essentially an indefinite period and querying those records constituted a continuing seizure. In *Ganias*, the Second Circuit addressed a limited issue, "whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize

and indefinitely retain every file on that computer for use in future criminal investigations," 755 F.3d at 137, and held that the lack of any limiting principle in such retention and review transformed what had initially been a valid search and seizure into an impermissible "general warrant." *Id*.

D. The NSA Program's Collection, Aggregation, Retention, and Review of Moalin's Telephone Metadata Violated the Fourth Amendment Because It Was Conducted Without Either a Warrant or Probable Cause.

Because the NSA program constituted a search and seizure of Moalin's call records without a warrant drawn with particularity and supported by probable cause, it violated the Fourth Amendment. Warrantless searches are "per se unreasonable," subject only to a few "jealously and carefully drawn exceptions." *Coolidge v. New Hampshire*, 403 U.S. 443, 545–55 (1971) (quotation marks omitted).

None of those "well-delineated exceptions" applies in this case. For that reason, no further analysis concerning "reasonableness" is necessary. *See Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 990 (9th Cir. 2011), quoting *Katz*, 389 U.S. at 357.

Indeed, the district court did not cite any exceptions to the warrant requirement in denying Moalin's post-trial motions. (As noted **ante**, the district court did not reach the merits of the issue because it held that Moalin did not possess a reasonable

expectation of privacy in his telephone call records.)[41]

The search and seizure of Moalin's highly personal information here was predicated on, in essence, a "general warrant" in the form of the FISC's blanket order for *all* call records, which renders the search and seizure *per se* unconstitutional. *See Berger v. New York*, 388 U.S. 41, 59 (1967). The subsequent aggregation, retention, and review of Moalin's call records similarly replicated in principle the evils of the notorious "general warrant."

As this Court has declared, "the wholesale seizure for later detailed examination of records not described in a warrant" is exactly "'the kind of investigatory dragnet'" the Fourth Amendment prohibits. *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (emphasis removed), quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980); *see Ganias*, 755 F.3d at 134-35 (Fourth Amendment "restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item

41 Elsewhere, the government has argued that the warrant requirement does not apply to the call-records program because the program serves special government needs. However, the "special needs" doctrine applies "[o]nly in those exceptional circumstances in which special needs, *beyond the normal need for law enforcement*, make the warrant and probable-cause requirement *impracticable*." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (emphases added); *see also Ferguson v. Charleston*, 532 U.S. 67, 81-86 (2001); *City of Indianapolis v. Edmond*, 531 U.S. 32, 41-47 (2000). Special-needs searches are confined to a "closely guarded category" permitted only "[i]n limited circumstances." *Chandler v. Miller*, 520 U.S. 305, 309, 314 (1997). Those circumstances are not present here.

not described in the warrant.").

Thus, in *United States v. Kow*, 58 F.3d 423 (9th Cir. 1985), this Court determined that a search warrant that "contained no limitations on which documents . . . could be seized or suggested how they related to specific criminal activity" failed the satisfy the Fourth Amendment's particularity requirement. *Id.* at 427. The Court held that the "generalized seizure" of a large collection of documents may be justified only on a showing of probable cause that the entire collection was likely to show evidence of criminal activity." *Id.*[42]

Here, with respect to Moalin, the NSA program operated as a general warrant for the digital age. Rather than setting out to obtain records *containing* evidence of criminal activity, the program gathered Moalin's records prospectively, "*hoping to find* among [those records] evidence of criminal activity" at some *future* point in time through retrospective searches of the data gathered already. *Ganias*, 755 F.3d at 134 (emphasis added); *see also ACLU v. Clapper*, 785 F.3d at 812.

That collection, aggregation, retention, and review process was wholesale and unlimited because the government acquired Moalin's complete call records – and,

42 Moreover, the exceptions simply prove the rule. *See Ganias*, 755 F.3d at 135 ("[c]ertain exceptions have been made in those 'comparatively rare instances where documents [we]re so intermingled that they [could not] feasibly be sorted on site.' But in those cases, the off-site review had to be monitored by a neutral magistrate and nonresponsive documents were to be returned after the relevant items were identified"), quoting *Tamura*, 694 F.2d at 595-97.

therefore, the highly detailed personal information revealed by those records, and then aggregated them with millions of others, thereby amplifying the constitutional speculative and untethered nature of the seizure and subsequent search(es).

As the Second Circuit found in *ACLU v. Clapper* in the statutory context, but equally applicable here in the constitutional sense, the government's demand for call records lacked *any* particularity. Nor was there *any* showing prior to collection that Moalin's call records contained information about terrorist or criminal activity, much less any showing that would amount to individualized suspicion. *See ACLU v. Clapper*, 785 F.3d at 812 (the "unprecedented and unwarranted" program enables the government, only "at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information" about particular individuals); *id.* at 813 ("[t]he records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subjects, or of people or businesses that have contact with others who are in contact with the subjects—they extend to every record that exists, and indeed to records that do not *yet* exist, as they impose a continuing obligation on the recipient of the subpoena to provide such records on an ongoing basis as they are created"). Moreover, here Moalin was *cleared* in the 2003 investigation, thus eliminating the "relevance" of any such records to any continuing or articulable investigation.

Thus, like a general search, the NSA program involved repeated searches and ongoing seizures of Moalin's telephone metadata not predicated upon "an oath or affirmation supplying cause." Morgan Cloud, *Searching Through History; Searching For History*, 63 U. Chi. L. Rev. 1707, 1738 (1996); *see Stanford*, 379 U.S. at 481; *see also* 50 U.S.C. §1861(b)(2)(a) (requiring only a "showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized [foreign-intelligence] investigation").

The NSA program was "not restricted to searches of specific places or to seizures of specific goods." Cloud, 63 U. Chi. L. at 1738; *see also Berger*, 388 U.S. at 59 (striking down electronic-surveillance statute that, like "general warrants," left "too much discretion of the officer executing the order" and gave the government "a roving commission to seize any and all conversations") (quotation marks omitted).

Accordingly, the warrantless search and seizure of Moalin's telephone metadata violated the Fourth Amendment.

E. The NSA Program's Long-term Collection, Aggregation, Retention, and Review of Moalin's Telephone Metadata Was Unreasonable.

Even if some exception to the warrant and probable-cause requirements applied, the NSA program exercised against Moalin's telephone metadata was unconstitutional because it was unreasonable under the Fourth Amendment.

Reasonableness is determined by examining the "totality of the circumstances" to "assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see Virginia v. Moore*, 553 U.S. 164, 169 (2008).

In the context of government surveillance, this test demands that statutes be "precise and discriminate" and that the government's surveillance authority be "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger*, 388 U.S. at 58. The NSA program as it was applied to Moalin – in which the government employed the most indiscriminate means possible quantitatively, qualitatively, and temporally to pursue its stated limited purpose of tracking the associations of a discrete number of suspected terrorists – cannot satisfy that burden.

As an initial matter, the intrusion here was far from minimal; it was extraordinary. The government collected records of Moalin's phone calls, then mingled that information with that of millions of others – records that contain a wealth of information, including medical, religious, romantic, familial, and political information – that were every bit as revealing as the content of calls. *See* PCLOB Report 12, 156-58; PRG Report 110-14, 116-17. *See also Clapper*, 785 F.3d at ------

*2; *Klayman*, 957 F. Supp. 2d at 33–37, 39, *vacated and remanded on other grounds*, ___ F.3d ___, 2015 WL 5058403 (D.C. Cir. August 28, 2015).[43]

Moalin's privacy interest in the intimate details of his personal life is not minimal; indeeed it lies at the very heart of what the Fourth Amendment is designed to protect. The program also lacks any of the traditional indicia of reasonableness under the Fourth Amendment. The government collected all of Moalin's call records without individualized suspicion, without temporal limit, and without limitation as to the individuals or phone calls swept up in the collection. *See, e.g.*, *Berger*, 388 U.S. at 55-56, 59-60 (invalidating surveillance statute due to the breadth, lack of particularity, and indefinite duration of the surveillance it authorized); *Chandler*, 520 U.S. at 313 ("[t]o be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing."); *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (FISA's requirement of individualized suspicion that the government's target is an "agent of a foreign power" is part of what makes it "reasonable."); *United States v. Tortorello*, 480 F.2d 764, 773–74 (2d Cir. 1973) (Title III provides for "particularity in the application and order" and "clearly circumscribe[s] the discretion" of the government "as to when the surveillance should

[43] In *Graham*, a case involving the government's warrantless collection of revelatory metadata, the Fourth Circuit recently held that "the government's procurement of the historical [cell site location information] at issue in this case was an unreasonable search." 796 F.3d F.3d at 359-60.

end."); *United States v. Cafero*, 473 F.2d 489, 498 (3d Cir. 1973) (similar); *In re Sealed Case*, 310 F.3d 717, 739-40 (FISCR 2002) (describing "constitutionally significant" limitations on the government's search powers).

Because the NSA program constituted a search and seizure of Moalin's call records without a warrant drawn with particularity and supported by probable cause, it violated the Fourth Amendment. Warrantless searches are "per se unreasonable," subject only to a few "jealously and carefully drawn exceptions." *Coolidge v. New Hampshire*, 403 U.S. at 545–55 (quotation marks omitted).

None of those "well-delineated exceptions" applies in this case. For that reason, no further analysis concerning "reasonableness" is necessary. *See Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 990 (9th Cir. 2011), quoting *Katz*, 389 U.S. at 357.

Indeed, the district court did not cite any exceptions to the warrant requirement in denying Moalin's post-trial motions. (As noted **ante**, the district court did not reach the merits of the issue because it held that Moalin did not possess a reasonable expectation of privacy in his telephone call records.)

As the collection, aggregation, retention, and review of Moalin's call records exemplifies, the NSA program also swept far more broadly than necessary to achieve the government's goals. The government's stated interest was in identifying unknown

terrorist operatives and thereby preventing terrorist attacks. *See, e.g.*, Br. for Appellees at 60, *Smith v. Obama*, No. 14-35555 (9th Cir. Oct. 2, 2014), ECF No. 55-1.

However, independent observers (that have been afforded broad access to the government's secret programs) agree that the NSA program did not achieve that objective. *See, e.g., Klayman*, 957 F. Supp. 2d at 40 ("the Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature"); Press Release, Sen. Ron Wyden, Wyden Statement on President Obama's Proposed Reforms to the FISC and PATRIOT Act (Aug. 9, 2013), http://1.usa.gov/1bBEyWb ("I have seen absolutely zero evidence that the bulk collection of Americans' phone records under Section 215 of the PATRIOT Act has provided any unique value to intelligence gathering or actually made Americans any safer . . . ."); PRG Report 118-19 (concluding that "there are alternative ways for the government to achieve its legitimate goals, while significantly limiting the invasion of privacy and the risk of government abuse"); PCLOB Report at 146 ("we have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records").[44]

[44] *See also* Siobhan Gorman, *NSA Chief Opens Door to Narrower Data Collection*, *The Wall Street Journal*, February 27, 2014, available at

Perhaps even more significantly, the modifications to the NSA program since it was used against Moalin, including most important this year's Congressional amendment of the enabling statute, demonstrate that those who have authorized and administered the NSA program are convinced the government can achieve its goal without the type of collection, aggregation, retention, and review to which Moalin's call records were subjected.

Also, as this Court has pointed out, although "the government's interest in preventing terrorism . . . is extremely high," the importance of that interest "is no excuse for the dispensing altogether with domestic persons' constitutional rights." *Al Haramain*, 686 F.3d at 993; *see also United States v. U.S. District Court (Keith)*, 407 U.S. at 316-21 (rejecting government's argument that national security required dispensing with the warrant requirement in domestic security surveillance cases).

Allowing even legitimate national security concerns to override the most fundamental of Fourth Amendment protections – the prohibition on the modern-day equivalent of the despised "general warrant" – would turn the Constitution on its head and destroy the basic civil liberties that the Founders fought to protect. For all those reasons, the totality of the circumstances demonstrates that the NSA program was

---

<http://on.wsj.com/1cA6SIr> ("[b]ut Gen. Alexander instead signaled that the information the NSA needs about terrorist connections might be obtainable without first collecting what officials have termed 'the whole haystack' of U.S. phone data").

unreasonable in its collection, aggregation, retention, and review of Moalin's telephone metadata.

F. The Evidence Derived from the NSA Program's Collection, Aggregation, Retention, and Review of Mr. Moalin's Telephone Metadata Should Have Been Suppressed As the Fruit of an Unlawful and/or Unconstitutional Search and Seizure, and Dismissal Is Also an Appropriate Remedy.

For more than a century, the federal courts have vigilantly enforced the remedy of suppression for violations of the Fourth Amendment for a simple reason: without it, the Fourth Amendment would be "reduce[d] . . . to a form of words." *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920) (Holmes, J.).

Thus, the purpose of the exclusionary rule is "to deter – to compel respect for the constitutional guaranty in the only effective available away – by removing the incentive to disregard it." *Elkins v. United States*, 364 U.S. 206, 217 (1960). Thus, under the rule, evidence obtained during or derived from an unconstitutional search may be so tainted by the illegality so as to render it inadmissible as "fruit of the poisonous tree." *See Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *see also New York v. Harris*, 495 U.S. 14, 19 (1980) (reaffirming "the familiar proposition that the indirect fruits of an illegal search or arrest should be suppressed when they bear a sufficiently close relationship to the underlying illegality"); *Chandler v. U.S. Army*, 125 F.3d 1296, 1304 (9th Cir. 1997).

Because the NSA program worked a "substantial and deliberate" violation of Moalin's Fourth Amendment rights, *Franks v. Delaware*, 438 U.S. 154, 171 (1978), the evidence obtained under the program – and both its direct and indirect "fruits," *i.e.*, essentially, the entirety of the government's evidence at trial, in the form of the recordings of Mr. Moalin's telephone conversations intercepted pursuant to FISA – should have been suppressed.

The government's use of the NSA program in this case demands application of the exclusionary rule for five reasons. First, the government's public statements make clear that the NSA program was the sole origin of the re-investigation of Mr. Moalin that led to the collection of all of the evidence that played a role in his prosecution and conviction. *See Hudson v. Michigan*, 547 U.S. 586, 592 (2006) ("but-for causality is only a necessary, not a sufficient, condition for suppression"); *United States v. Crews*, 445 U.S. 463, 471 (1980) (causation analysis inquires whether "the challenged evidence is in some sense the product of illegal government activity"). Sean Joyce, Deputy Director of the FBI, told the House Permanent Select Committee on Intelligence ("HPSCI") that "the NSA, using the business records FISA, tipped us off that this individual" – unmistakably Moalin – "had indirect contacts with a known terrorist overseas." (CR 345-2 at 9-10.) As a result of this "tip," obtained via the call-records program, the government was "able to reopen th[e] investigation" of Moalin,

– an investigation that, in 2003, "did not find any connection to terrorist activity" – by "serv[ing] legal process to identify" Moalin and to obtain orders from the FISC for electronic surveillance under FISA. *Id*.

In publicly defending its call-records program, government officials have told this story numerous times, with little variation. Each time, the government has made clear that without the unconstitutional NSA program, the investigation of Moalin would not have been reignited. The rationale of the exclusionary rule includes the principle that "the prosecution is not to be put in a better position than it would have been in if no illegality had transpired." *Nix v. Williams*, 467 U.S. 431, 433 (1984). But without the illegality in this case, there would not even have been an *investigation*, much less a prosecution.

Second, the government's evidence is not "so attenuated . . . so as to remove the 'taint' imposed upon that evidence by the original illegality." *Crews*, 445 U.S. at 471; *see Nardone v. United States*, 308 U.S. 338, 341 (1939). As the Supreme Court has instructed, "[t]he notion of the 'dissipation of the taint' attempts to mark the point at which the detrimental consequences of illegal police action become so attenuated that the deterrent effect of the exclusionary rule no longer justifies its cost." *Brown v. Illinois,* 422 U.S. 590, 609 (1975) (Powell, J., concurring); *see Wong Sun*, 371 U.S. at 488 ("the more apt question in such a case is whether, granting establishment of the

primary illegality, the evidence to which instant objection is made has been come at *by exploitation of that illegality* or instead by means sufficiently distinguishable to be purged of the primary taint") (emphasis added) (quotation marks omitted); *Segura v. United States*, 468 U.S. 796, 804 (1984); *United States v. Perez-Castro*, 606 F.2d 251, 253 (9th Cir. 1979).

In cases in which this Court addresses evidence obtained indirectly, as here, the Court has "stated the test to be whether the illegal activity tends to *significantly direct the investigation* to the evidence in question." *United States v. Chamberlin,* 6 44 F.2d 1262, 1269 (9th Cir. 1980) (emphasis added) (citations omitted); *see United States v. Davis,* 332 F.3d 1163, 1171 (9th Cir. 2003); *United States v. Foppe*, 993 F.2d 1444, 1449 (9th Cir. 1993).

Also, when determining attenuation, "temporal proximity . . . , the presence of intervening circumstances, and, particularly, the purpose and flagrancy of the official misconduct are all relevant." *Brown*, 422 U.S. at 603–04 (footnotes and citations omitted); *see United States v. Shephard*, 21 F.3d 933, 939 (9th Cir. 1994).

Here, the "direction" the NSA program's violations provided to the investigation was not merely "significant" – it was *indispensable*. *Chamberlin*, 644 F.2d at 1269. Also, there can be little question that the government's evidence in this case came "by exploitation of the primary illegality," *Wong Sun*, 371 U.S. at 488

(quotation marks omitted) – *i.e.*, the NSA program.

By the government's own account, it obtained subpoenas and FISA warrants using the information gathered about Moalin through the NSA program. *See Shephard*, 21 F.3d at 939 ("[t]he closer the link between the illegal arrest and the seizure, the more likely we are to conclude that there is 'exploitation' of the arrest by the police").

Moreover, any intervening circumstances to which the government might point – including later use of different legal authorities to continue the investigation of Moalin – cannot cleanse the taint from the NSA program. *See, e.g.*, *United States v. Perez*, 506 F. App'x 672, 674-75 (9th Cir. 2013) (remanding for consideration of suppression of evidence obtained at defendant's home when "officers' suspicion . . . seems to have arisen, at least in part, as a result of their seeing . . . incriminating photographs and text messages" obtained through an illegal search); *United States v. Thomas*, 211 F.3d 1186, 1192 (9th Cir. 2000) (requiring suppression of marijuana found in defendant's home as the result of information acquired during unconstitutional traffic stop); *Commonwealth v. Keefner*, 461 Mass. 507, 518 (2012) (affirming suppression of evidence acquired after unlawful search of text messages led to additional investigatory paths); *Staples v. United States*, 320 F.2d 817, 820 (5th Cir. 1963) (requiring suppression of evidence obtained in hotel room to which

key was found through an unlawful search of defendant's car).

Third, excluding the evidence derived from the NSA program here would fulfil the purpose of the "fruit of the poisonous tree" doctrine to protect the "integrity or fairness of a criminal trial." *Nix v. Williams*, 467 U.S. at 446; *see also I.N.S. v. Lopez-Mendoza*, 468 U.S. 1032, 1050 (1984) (suppression warranted when government effectuates "egregious violations of Fourth Amendment or other liberties that might transgress notions of fundamental fairness").

Moalin was indicted October 22, 2010, and he was convicted after a jury trial that concluded February 22, 2013. Yet Moalin did not learn of the role that the call-records program played in his investigation and prosecution until after *June 18, 2013* – while awaiting sentencing – and then only fortuitously when Sean Joyce appeared before the HPSCI to defend the NSA program in the wake of Mr. Snowden's disclosures, and to claim this case as the call-records' program's only success story to date.

The failure of the government to notify Moalin about the role the NSA program played in his investigation and prosecution (and conviction) offends basic constitutional notions of "integrity and fairness" in criminal trials. *See, e.g., Lambert v. California*, 355 U.S. 225, 228 (1957) ("[e]ngrained in our concept of due process is the requirement of notice. Notice is sometimes essential so that the citizen has the

chance to defend charges"); *United States v. Gomez*, 191 F.3d 1214, 1220 (10th Cir. 1999) ("'[t]he central concern of the Confrontation Clause is to ensure the reliability of the evidence against a criminal defendant by subjecting it to rigorous testing in the context of an adversary proceeding before the trier of fact'"), quoting *Lilly v. Virginia*, 527 U.S. 116 (1999) (plurality op.)[45]

In addition, the government's withholding of notice of electronic surveillance is now widespread. *See generally* Patrick C. Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 Santa Clara L. Rev. 843, 865–895 (2014). Excluding the evidence derived from the call-records program in Moalin's case could promote the values of fundamental fairness and systemic integrity that animate the constitutional guarantees to criminal defendants in our system. *See Nix*, 467 U.S. at 446 (suppression warranted where it "safeguard[s] the adversary system of justice").

Fourth, "the deterrence benefits of suppression" here "outweigh" the costs. *Davis v. United States*, ---- U.S. ----, 131 S. Ct. 2419, 2427 (2011). As the Supreme Court explained in *Davis*, "the deterrence benefits of exclusion 'var[y] with the culpability of the law enforcement conduct' at issue." *Id.* (alteration in original),

---

45 This failure is only compounded by the District Court's errors in refusing additional disclosure of evidence and exculpatory material to Moalin during trial as explained in argument III.

quoting *Herring v. United States*, 555 U.S. 135, 143 (2009). The NSA program operated – first under unilateral presidential authorization, and then under secret orders of the FISC – with near impunity for more than a decade. This is the very first criminal prosecution in which information derived from the NSA program has been subject to challenge. The NSA program has "exhibit[ed] 'deliberate,' 'reckless,' [and] 'grossly negligent' disregard for Fourth Amendment rights," *id.* quoting *Herring*, 555 U.S. at 1444, with no recourse for – or even knowledge by – Mr. Moalin or the millions of Americans whose sensitive and private information scooped up by the NSA program. *See Lopez-Mendoza*, 468 U.S. at 1050 (denying suppression but explaining that "[o]ur conclusions concerning the exclusionary rule's value might change[] if there developed good reason to believe that Fourth Amendment violations . . . were widespread"); *United States v. Roberts*, 779 F.2d 565, 568 (9th Cir. 1986) (suppression would be appropriate in the face of "widespread and repeated violations") (quotation marks omitted).

Here, the Fourth Amendment violations were not merely "widespread and repeated," but, as the review of it in *ACLU v. Clapper* (in the context of the analysis of the statutory violation) demonstrates, *they were built into the very architecture of the program*. Unlimited in time, quantity, and utility, the NSA program constituted a guaranteed continuing Fourth Amendment violation perpetrated against all

Americans.

Moreover, while the statutory authority on which the program has most recently been based no longer exists, a future administration might well revert to prior legal theories to restart the program – unless this Court exercises its "'judicially created' sanction," *Davis*, 131 S. Ct. at 2433, quoting *Calandra*, 414 U.S. at 348, and deters such future unconstitutional conduct through application of the exclusionary rule.[46]

Fifth, and finally, the principal exceptions to the exclusionary rule – the independent-source rule and the good-faith exception – are inapplicable here. The "independent source doctrine allows admission of evidence that has been discovered by means wholly independent of any constitutional violation." *Nix*, 467 U.S. at 443. However, as discussed above, the constitutional violation in this case was the *lone* source of evidence in the reopening of the investigation of Mr. Moalin, and in generating the evidence for his prosecution.

---

[46] While the deterrent value of suppression in this case is at its apex, the "principal cost of applying the rule" in this case, *Herring*, 555 U.S. at 141 – "letting guilty and possibly dangerous defendants go free," *id.* – is small. However serious the alleged conduct is in this case, and even assuming the accuracy of the verdict, even the District Court at sentencing noted, with to the three defendants sentenced that day (all of whom have now been in custody since October 2010) that "[w]hen it comes to specific deterrence I don't think we need worry about any of these three gentlemen." (Sent. Trans. at 130.) Furthermore, the Supreme Court has instructed that however disfavored suppression is as a remedy for constitutional violations, "society must swallow this bitter pill when necessary." *Hudson*, 547 U.S. at 591.

That the government may have utilized other legal authorities in its investigation after violating Moalin's rights through the NSA program does not render those means "independent" for the purposes of the exclusionary rule unless the later authorities were "unrelated" to the information acquired through the NSA program. *United States v. Ramirez-Sandoval*, 872 F.2d 1392, 1396 (9th Cir. 1989). Far from unrelated, the NSA program was indispensable to the government's later use of different authorities to conduct surveillance of Mr. Moalin..[47] Moreover, the good-faith exception to the exclusionary rule does not apply to cases in which "the law governing the constitutionality of a particular search is unsettled." *Davis*, 131 S. Ct. at 2435 (Sotomayor, J., concurring). As discussed previoulsy, *Smith v. Maryland* cannot bear the precedential weight that the government assigns to it in these circumstances and the Circuit decisions in *ACLU v. Clapper*, *Graham*, and even *Klayman* (in which the plaintiffs' standing was not rejected categorically due to *Smith*) demonstrate as much. This is decidedly not a case in which "binding appellate

---

47 The Supreme Court has explained that another exception, the "inevitable discovery" doctrine, "is in reality an extrapolation from the independent source doctrine: *since* the tainted evidence would be admissible if in fact discovered through an independent source, it should be admissible if it inevitably would have been discovered." *Murray v. United States*, 487 U.S. 533, 539 (1988) (emphasis in original.) Here, the government has not even attempted to argue that the "inevitable discovery" doctrine would apply to the investigation of Moalin, and its public statements regarding the importance of the NSA program to the revival of that investigation foreclose it.

precedent specifically *authorizes* a particular police practice[.]" *Davis*, 131 S. Ct. at 2429. Consequently, the good-faith doctrine is inapplicable here.

Finally, in addition to suppression of evidence, dismissal of the Indictment as to all Appellants is an appropriate remedy. *See Chapman*, 524 F.3d at 1084-88.

G. All Appellants Have Standing for the FISA Claims.

Appellants Mohamud, Doreh, and Nasir also have "standing" to challenge the telephone metadata program. Under the plain language of FISA, "[a]ny person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person . . . may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that – (1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval." 50 U.S.C. § 1806(e). There is no question that Appellants Mohamud, Doreh, and Nasir are "aggrieved persons," as their conversations were intercepted pursuant to the FISA warrant, and an "aggrieved person" means "any person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). Accordingly, they are permitted to make a claim that such information "was unlawfully acquired . . . ." 50 U.S.C. § 1806(e).

The use of the "information was unlawfully acquired" language in section 1806(e) is different and more broad than the language used in Title III, and it is

presumed that Congress acted intentionally when it incorporated the different language. *See Custis v. United States*, 511 U.S. 485, 492 (1994); *see also Dean v. United States*, 556 U.S. 568, 573 (2009) (quoting *Russello v. United States*, 464 U.S. 16, 23 (1983)). Under Title III, an "aggrieved person" may move to suppress the contents of an intercepted communication "on the grounds that – (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval." 18 U.S.C. § 2518(10)(a). Thus, an aggrieved person may only move to suppress under Title III if a particular "communication" was "unlawfully intercepted," whereas an aggrieved person may move to suppress under FISA if "information" was "unlawfully acquired." As argued earlier in this brief, and as confirmed in *Clapper*, all of the information obtained pursuant to the FISA warrant had an unlawful genesis and therefore was "unlawfully acquired."

Furthermore, like Moalin, all of the Appellants were subjected to the unlawful telephone metadata program. As explained in *Clapper*, their metadata information, like the information of tens of millions of others, was "seized" pursuant to the unlawful program. In other words, they are "aggrieved persons" of the unlawful metadata program. They therefore have "standing" to assert the program's illegality

as a basis for a motion to suppress. *Cf. Clapper*, 785 F.3d at 801-02 (the mere collection of the metadata constitutes a "seizure" that bestowed standing).

III.

THE CONVICTIONS SHOULD BE VACATED AND A NEW TRIAL ORDERED BECAUSE THE GOVERNMENT FAILED TO PRODUCE EXCULPATORY INFORMATION AND/OR PROVIDE NOTICE OF ITS SURVEILLANCE ACTIVITIES.

The revelation of the implementation of the NSA's bulk telephone metadata collection against Moalin also confirmed that the government had failed to disclose to the defense certain exculpatory information that the government was obligated to produce pursuant to the Fifth Amendment's Due Process clause and *Brady v. Maryland*, 373 US. 83 (1963). As a result, the convictions should be vacated and a new trial ordered.

In fact, Moalin moved pretrial for disclosure of certain *Brady* material that was clearly implicated by the FBI's FIG Assessment (CR 92), but which the government refused to provide, and which the trial court declined to order the government to produce. (CR 124.)

As detailed below, at trial other documents, including an FBI personality profile of Moalin, produced pursuant to 18 U.S.C. §3500 only two days prior to trial, provided additional exculpatory evidence that, while used during cross-examination

of the government's Somali linguist, could not be exploited effectively because of its disclosure on the eve of trial.

Post-trial, the disclosure of how the government's collection, aggregation, retention, and review of Moalin's telephone metadata precipitated a renewed investigation of him, leading to the FISA electronic surveillance, not only revealed slightly more of that exculpatory information, but also amply reinforced the importance of the still undisclosed information underlying the FIG Assessment and the personality profile. Thus, again Moalin moved for disclosure of *Brady* material, but was again rebuffed by the government and denied by the district court.

However, as set forth below, in aggregate that exculpatory information – much of which the government has still not disclosed – was certainly material, as it was entirely consistent with, and demonstrative of, Moalin's defense that he did not provide any funds with the intent to assist al-Shabaab, but only to provide relief, in various forms, for his native region in Somalia, and/or based on clan affiliation and ambitions.

Also, in light of the post-trial disclosures, it may very well have cast significant doubt – even reasonable doubt – on the essence of the government's theory of prosecution: that Moalin was in *direct* contact with any member of al-Shabaab.

In addition, relatedly, the government failed to provide the defendants notice

of NSA's bulk collection of Moalin's telephone metadata. That dereliction denied defendants Due Process, as it deprived them of the opportunity to challenge the collection, retention, aggregation, and review of that metadata, and its contributions to the government's acquisition of evidence used against defendants at trial.

A. Definition of *Brady* material.

To prove a *Brady* violation Appellants must show that the government failed to disclose material evidence. Evidence is material "if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *United States v. Bagley*, 473 U.S. 667, 682 (1985).

B. Preserved Error: Appellants Repeatedly Requested *Brady* Materials.

1. Pretrial Motions

More than a year before trial, the defense made specific *Brady* requests for two discrete purposes: (1) to challenge the FISA electronic surveillance conducted on Moalin, and which also intercepted the communications of M. Mohamud, Doreh, and Nasir Mohamud; and (2) for use at trial to refute the government's case.

Regarding the former, the defense moved pursuant to 50 U.S.C. §1806(f), which authorizes a court to "disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other

materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance[,]" and §1806(g), which expressly incorporates the Fifth Amendment Due Process Clause, and provides that "[i]f the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person *except to the extent that due process requires discovery or disclosure*." 50 U.S.C. §1806(g) (emphasis added). *See also United States v. Spanjol*, 720 F. Supp. 55, 57 (E.D. Pa. 1989) ("[u]nder FISA, defendants are permitted discovery of materials only to the extent required by due process. That has been interpreted as requiring production of materials mandated by [*Brady*], essentially exculpatory materials").

Regarding the material's relevance to Moalin's (and his co-defendants') defense, the FIG Assessment establishes that exculpatory material and information that exists was not produced to the defense, but which should have been provided pursuant to *Brady*. The FIG Assessment was prepared "to document San Diego FIG [Field Intelligence Group] assessment of Basaaly Moalin's motivation for providing financial support to al-Shabaab circa April, 2009." (CR 345-1.)

In fact, the investigation of Moalin that resulted in this prosecution commenced December 18, 2007. (*Id*.) The primary investigative tool was electronic surveillance of Moalin's telephone and e-mail account, both authorized pursuant to FISA. The

discovery provided by the government showed the earliest wiretapped conversations occurred December 20, 2007, and the last were December 2, 2008. Also during 2008, the FBI conducted periodic physical surveillance of Moalin.

Following termination of the physical and electronic surveillance of Moalin, the FBI San Diego Field Intelligence Group issued an assessment of his "motivation for providing financial support to al-Shabaab." (*Id*.)

The FIG Assessment reports that "[o]n 4/23/2009, as per *the referenced document*, the San Diego Field Intelligence Group (FIG) provided the following assessment of Basaaly Moalin's possible motivation for providing financial support to al-Shabaab in Somalia[.]" *Id*. (emphasis added). Thus, the FIG Assessment itself refers to another document that contains information related to that in the FIG Assessment, but which was not produced, notwithstanding the defense's specific request for it.

Also, the FIG Assessment notes, *inter alia*, that:

- "[a]lthough Moalin has previously expressed support for al-Shabaab, *he is likely more attentive to Ayr subclan issues and is not ideologically driven to support al-Shabaab*." *Id*. (emphasis added);

- "[t]he San Deigo FIG assesses that Moalin likely supported now deceased senior al-Shabaab leader Aden Hashi Ayrow *due to Ayrow's tribal affiliation with the Hawiye tribe/Habr Gedir clan/Ayr subclan rather than his position*

in al-Shabaab." *Id*. (emphasis added); and

- "*Moalin has also worked diligently to support Ayr issues to promote his own status with Habr Gedir elders*." *Id*. (emphasis added).

The italicized portions unmistakably constitute *Brady* material, and required the government to produce – as the defense requested pretrial – the following material and information relating to and underlying those quoted portions:

(1) any and all witnesses whose statements provided the basis for the italicized conclusions;

(2) any and all reports (however memorialized or stored) containing information or facts forming the basis for the italicized conclusions;

(3) any and all records and/or other documents (however memorialized or stored) containing information or facts forming the basis for the italicized conclusions;

(4) internal reports, memoranda, and/or analyses containing information, facts, or analysis forming the basis for the italicized conclusions; and

(5) surveillance materials – whether visual, audio, or otherwise (however created or stored) – containing information or facts forming the basis for the italicized conclusions.

Given that the FISA electronic surveillance ended in December 2008, but defendants were not indicted until October 2010, the defense also moved to compel the government to produce information, reports, memoranda, and/or other materials

reflecting whether the investigation against Moalin was at some point suspended, closed, or otherwise de-activated, and the reasons for such action. The government resisted all such requests, and the district court denied the defense motions to compel production.

2. The Production of Exculpatory 3500 Material on the Eve of Trial

Two days prior to the commencement of trial, the government produced, in the form of 3500 material, an October 2008 internal FBI personality profile of Moalin – prepared *after* the electronic surveillance had been underway for more than ten months – authored by the government's Somali linguist, Abdirahman Liban, who had listened to the intercepted telephone calls and reviewed Moalin's e-mails.

That personality profile noted the following:

- Moalin's "life goals" – "To be successful in Somali politics and become a wealthy businessman with many children and . . . to develop and enhance his home region in Somalia"
- Moalin's "stressors" – "Finances and not being able to build his dream home"
- Moalin was bothered by "[t]he suffering and destruction in Somalia caused by both the fighting and the drought" and
- Moalin was competitive – he "[w]ould try to outshine others in supporting his home region [Gelgaduud]"

(CR 370, Sent. Memo Moalin, at 32-33). Also, Abdirahman noted in a September 23,

2008, e-mail, with respect to a particular group of intercepted phone calls, again, at the conclusion of the investigation, that the "[s]essions have been about improving the condition of Gelgaduud region thus far[.]" That is consistent with Moalin's overriding goals, and his (and his co-defendants') defense. For example, in a conversation recorded April 12, 2008, Moalin replies that he is "doing well except the drought and the difficulties people are facing – and the fighting. . . . Which affected me financially and mentally." (6RT 1045, Gov. Exhibit 150.) On April 17, 2008, Moalin's message is that "we don't care for those who has political or clan agenda. Our intention is to provide help." (6RT 1056, 8RT1354; Gov. Exhibit 155, as augmented by TT-155; *see also* 7RT 1233; 6RT 1019, 1017; Gov. Exhibits 124, 131, and 134.)

While the information in the personality profile was used to limited extent as impeachment of Abdirahman during his cross-examination, its disclosure on the veritable eve of trial precluded any substantive use of the information. Nor did the government provide any of the supporting materials that influenced Abdirahman's conclusions.

The material produced pursuant to 18 U.S.C. §3500 for Abdirahman, (CR 370, Sent. Memo Moalin, at 32-33), also included a January 24, 2008, e-mail from a redacted source (probably FBI Special Agent Michael C. Kaiser, the case agent) that

stated, "We just heard from another agency that Ayrow tried to call Basaaly today, but the call didn't go through." This raises the additional question whether Moalin was subject to other means of interception, *i.e.*, Section 702 (FAA §1881a), conducted by NSA even while the FBI's FISA wiretap was underway.

3. Post-Trial Revelations

Of course, after trial the exculpatory disclosures continued, this time in the form of FBI Deputy Director Joyce's explanation that the FBI had conducted a prior investigation of Moalin "after 9/11" and "did not find any connection to terrorist activity." Deputy Director Joyce added that the NSA's bulk telephony metadata collection and retention program had established that Moalin "had indirect contacts with a known terrorist overseas." (CR 345-3.)

NSA Director General Alexander provided more details, including that:

- NSA reviewed a telephone number "associated with *al-Qaeda*,";
- NSA "looked at that phone number and we saw it touched a phone number in San Diego"; and
- NSA "saw [Moalin's telephone number] talking to a facilitator in Somalia" in 2007, which caused the FBI, when so informed, to reopen its investigation of Moalin.

The relevance of that information, whether individually or in aggregate, is manifest. For example, the 2003 investigation of Moalin "did not find any connection

to terrorist activity[,]" which echoes the FIG Assessment's conclusions. Yet none of the raw material enabling the defense to establish Moalin's lack of connection to terrorist activity was produced by the government. (CR 345-3 at 18.)

Also, Moalin's telephone number merely "touched" a number "associated with *al-Qaeda*[,]" which raises several questions, including: (1) what does "associated" with *al-Qaeda* mean? The government alleged Moalin was in contact with a specific principal of al-Shabaab – Aden Ayrow – and not someone simply (and vaguely) "associated" with *al-Qaeda*; (2) was Moalin's number in *direct* contact with that phone number, or was it a "hop" or *two* or *three* (or even more) away?

If Moalin was only in indirect contact with "extremists" overseas – as Deputy Director Joyce's and Director Alexander's remarks state – that would have struck a serious if not fatal blow to the government's claim – indispensable to its trial theory – that Moalin was conversing on the telephone directly with the military leader of al-Shabaab (Ayrow); and (3) similarly, if Moalin's telephone number was in contact with only a "facilitator in Somalia," how did that affect the government's claim that the other party to Moalin's conversations was *Aden Ayrow himself*?[48]

[48] Abdirahman's §3500 material also included an e-mail from FBI SA Kaiser in which SA Kaiser, in response to Abdirahman's query regarding why SA Kaiser thought "Sheikalow" – with whom Moalin was having telephone conversations – was Aden Ayrow, claimed that "Sheikalow" was merely a "slurred version of Sheikh Ayrow" – an assertion the government *never* posited at trial or at any point during the prosecution. (CR 345.)

As a result, in their post-trial motions Moalin and his co-defendants moved for production of *Brady* material in the form of:

> (a) the reasons underlying the conclusion, at the end of the initial 2003 investigation of Moalin, that he was not engaged in illegal conduct or linked to terrorism. Also, that earlier investigation likely yielded abundant if not conclusive evidence that Moalin was sending money to Somalia for humanitarian and other (family) purposes even before al-Shabaab existed, and that he did not harbor anti-U.S. or pro-terrorist sympathies;[49]
>
> (b) evidence that Moalin's contacts with al-Shabaab that precipitated renewal of the investigation were *in*direct, and not directly with Ayrow;
>
> (c) anything exculpatory generated by and during the earlier Anaheim investigation referred to in Ahmed Nasir's Pre-Sentence Report – which also resulted in a declination of charges; and
>
> (d) exculpatory information and material related to the FIG Assessment itself, which Moalin requested in his pretrial motions.

(CR 345 at 37-38; CR 361.)

The defense also demanded production – and that the government search for such materials and information – of not only the items enumerated above, but also any other exculpatory material and information reviewed in the process (as the

---

[49] The FIG Assessment was prepared in April 2009, while the initial investigation occurred years earlier (2003). As a result, the information from either might be in many ways distinct.

defense remained unaware of the specific nature and type of exculpatory information and material in the government's possession).

Again, the government resisted disclosure, and, again, the district court denied the defense's motion to compel. (CR 386.) Consequently, the defense has never had access to material exculpatory information it *knows* exists by the government's own admission, but which the government has steadfastly refused to provide.

C. The Principles Relevant to Evaluating a *Brady* Violation

As this Court explained in *United States v. Price*, 566 F.3d 900 (9th Cir. 2009),

> [t]here are three components of a *Brady* violation: "The evidence at issue must be favorable to the accused, either because it is exculpatory, or because it is impeaching; that evidence must have been suppressed by the State, either willfully or inadvertently; and prejudice must have ensued." *Strickler v. Greene,* 527 U.S. 263, 281-82 (1999).

566 F.3d at 907.

Also, as this Court instructed in *Price*,

> t]he term "suppression" does not describe merely overt or purposeful acts on the part of the prosecutor; sins of omission are equally within *Brady's* scope. *See Benn v. Lambert,* 283 F.3d 1040, 1053 (9th Cir.2002) ("[T]he terms 'suppression,' 'withholding,' and 'failure to disclose' have the same meaning for *Brady* purposes.").

566 F.3d at 907. *See also id*. at 907-08 ("w]e perform this step of the inquiry "irrespective of the good faith or bad faith of the prosecution" in failing to disclose

favorable evidence" because "an 'innocent' failure to disclose favorable evidence constitutes a *Brady* violation nonetheless") (footnote omitted), citing *Brady,* 373 U.S. at 877; *Edwards v. Ayers,* 542 F.3d 759, 768 (9th Cir. 2008) ("[s]uppression by the prosecution, whether willful or inadvertent, of evidence favorable to the accused and material to either guilt or punishment violates the Constitution); *United States v. Antonakeas*, 255 F.3d 714, 725 (9th Cir. 2001).

In addition, and relevant in the context of this case, in which the role of NSA's previously secret (and classified) bulk telephone metadata collection program may or may not have been known to the prosecuting attorneys, but was known to U.S. intelligence agencies (and intelligence personnel within the FBI), this Court in *Price* added that "[t]he Supreme Court has clearly held that '*Brady* suppression occurs when the government fails to turn over even evidence that is "known only to police investigators and not to the prosecutor."' 566 F.3d at 908 (internal citations and quotations omitted.)

Also resonating here in light of NSA's clandestine operation of the bulk telephone metadata program is this Court's comment in *Price* that

> . . . exculpatory evidence cannot be kept out of the hands of the defense just because the prosecutor does not have it, where an investigating agency does. That would undermine *Brady* by allowing the investigating agency to prevent production by keeping a report out of the prosecutor's hands until the agency decided the prosecutor ought to have it. . . .

566 F.3d at 908 (citations and quotations omitted) ("[b]ecause the prosecution is in a unique position to obtain information known to other agents of the government, *it may not be excused from disclosing what it does not know but could have learned*") (emphasis in original) (quotation omitted).

Price established procedures for analyzing *Brady* violations. The defendant must produce some evidence supporting an inference that the government possessed or knew of material favorable to the defense but did not disclose it. 566 F.3d at 910 (citations omitted.)

However, "[o]nce the defendant produces such evidence, the burden shifts to the government to demonstrate that the prosecutor satisfied his duty to disclose all favorable evidence known to him or that he could have learned from "'others acting on the government's behalf.'" 566 F.3d at 910 (quoting *Kyles v. Whitley*, 514 U.S. 419, 437 (1995). As a result, "[t]he suppression prong of *Brady* may be met, however, even though a 'record is not conclusive as to whether the individual prosecutor[or investigator] . . . ever actually possessed' the *Brady* material." 566 F.3d at 910, quoting *Carriger,* 132 F.3d 463, 479 (9th Cir.1997).

Regarding the third prong of the *Brady* analysis – whether the information qualifies as "material," *i.e*., "whether the failure to disclose the *Brady* material was prejudicial," 566 F.3d at 911 (footnote omitted) – this Court has observed that "'[t]he

touchstone of [the prejudice analysis] is whether admission of the suppressed evidence would have created a "reasonable probability of a different result.'" 566 F.3d at 911, quoting *United States v. Jernigan,* 492 F.3d 1050, 1053 (9th Cir.2007) (en banc) (quotation omitted)

This Court has also cautioned that "the Supreme Court has stressed [that] it has 'rejected a standard that would require the defendant to demonstrate that the evidence if disclosed probably would have resulted in acquittal." 566 F.3d at 911 (quotations and citations omitted.) The law only requires a "reasonable probability" which is "a probability sufficient to undermine confidence in the outcome"' of the trial. 566 F.3d at 911 (quotations and citations omitted).

This Court considers the context of the entire record in deciding whether undisclosed *Brady* materials undermines its confidence in the outcome of the trial. 566 F.3d at 913 (citations and quotations omitted.) However, *Brady* analysis is *not* a sufficiency test. *Paradis v. Arave*, 240 F.3d 1169, 1177 (9th Cir. 2001). Thus, whether the government's case satisfied the elements of the offense(s) is not determinative. Rather it is the impact of the information that was *not* disclosed to the defense, and consequently not presented to the jury for consideration, that is dispositive.

Brady extends to evidence that goes to punishment. *Bagley*, 473 U.S. at 683

(1985)(citation omitted) *see also United States v. Houston*, 648 F.3d 806, 813 (9th Cir. 2011) (due process requires that evidence be turned over by the prosecution if it is "exculpatory" or "impeaching" to the government's case).

Brady extends to material that supports a defendant's motion to suppress evidence. *United States v. Barton*, 995 F.2d 931, 935 (9th Cir. 1993) (holding that the "due process principles announced in *Brady* and its progeny" also apply to suppression hearings); *Smith v. Black*, 904 F.2d 950, 965–66 (5th Cir. 1990), *vacated on other grounds*, 503 U.S. 930 (1992) (due process mandates the disclosure of information in the government's possession if nondisclosure would "affect[] the outcome of [a] suppression hearing"); *see also United States v. Phillips*, 540 F.2d 319, 325–26 (8th Cir. 1976) (party seeking to suppress fruit of unlawful surveillance must be given a "full and fair opportunity" to meet *prima facie* burden of showing that the surveillance was unlawful).

D. The Exculpatory Material Produced By the Government Was Incomplete and Inadequate to Satisfy Its *Brady* Obligations

Requests for *Brady* material often occur in a partial vacuum: because the government possesses the information and materials, more often than not defendants can only propose subject matters of exculpatory material and information that might exist without firm knowledge of whether it, or in what form, it exists at all. As a

result, courts, too, are not usually in a position to identify exculpatory material and information with precision, and instead are limited to reminding the government of its obligation to provide *Brady* material, and deferring to and relying upon the government's recognition of that constitutional duty.

However, here defendants and the Court are aware of specific *Brady* material that has existed since the case began, but which the government did not produce, namely, the underlying bases for the FIG Assessment, the 2008 FBI personality profile, and the Section 215 interception/collection and the underlying information related to the previously terminated investigation of Moalin (that may have contributed to the conclusions noted in the FIG Assessment and personality profile).

While still unable to identify the exact form in which such exculpatory material and information exists, defendants did to some extent, (CR 92, 345), to articulate its nature. Nevertheless, the opaque nature of the redacted FIG Assessment, and the statements by Deputy Director Joyce and General Alexander, do not provide the defense any capacity to be more specific, or to have (with respect to the FIG Assessment, the only information provided sufficiently prior to trial) developed the underlying sources as witnesses and/or evidence at trial. An additional impediment to any defense attempts to pursue the information further is that it may well be that the information was and/or remains classified in some respect.

In the district court, the government's opposition to the defense's request for exculpatory material referred to in the FBI FIG assessment misapprehended the nature of what constitutes exculpatory material under *Brady* and its progeny, as well as the extent of the government's obligation to produce such information to the defense.

For example, in claiming that the FIG is not exculpatory because it also contains inculpatory information, (CR 108, at 14), the government fails to recognize the nature of *Brady* material. Even assuming *arguendo* that the FIG as a whole is inculpatory, a document is not analyzed *en toto* to determine whether it is on balance exculpatory or inculpatory. Rather, exculpatory information *within* a document is *Brady* material regardless of the overriding character of the document, or whether the document also contains *in*culpatory aspects. *United States v. Howell*, 231 F.3d 615, 625 (9th Cir. 2000) ("[t]hat the information withheld may seem inculpatory on its face in no way eliminates or diminishes the government's duty to disclose evidence of a flawed police investigation").

The reasons for the government's refusal to acknowledge that the FBI's FIG Assessment constituted *Brady* material[50] are sufficiently obvious that they need not

---

50 If the FIG Assessment was not *Brady* material, that begs the question: why was it produced pretrial at all? An internal government investigative analysis, it certainly was not discoverable pursuant to Federal Rule of Criminal Procedure 16.

be explained further. However, that does not excuse it, or alter the facts. Indeed, the *NACDL Report*, which reviewed 620 decisions deciding the merits of an alleged *Brady* violation, found that "[t]he judiciary's almost unilateral focus on materiality conveys a message that non-material favorable information is unimportant and need not be disclosed. As a result, the current system of judicial review fails to promote a culture of compliance, instead fostering *Brady*, or 'so-called *Brady*,' violations." *NACDL Report*, at 44.[51]

As a result, the *NACDL Report* concluded, regardless of whether the courts found a *Brady* violation (which they hardly ever did), the "important point is that valuable information that could have helped bolster the defense theory, led to a more effective trial strategy, or led to other material information was not turned over to the defense." *Id*. at 42.

---

[51] As the *NACDL Report* points out, prosecutors' inability to recognize the character of material and information they have a duty to disclose is at odds with their ethical obligations, but nevertheless fostered by prosecutorial doctrine that is in conflict with those ethical duties. While courts have "been reminding prosecutors all along that they are ethically bound under professional rules to a broader disclosure obligation beyond what the Constitution provides a defendant[,]" *NACDL Report*, at 8, citing ABA Formal Opinion 09-454 ("requires the disclosure of evidence or information favorable to the defense without regard to the anticipated impact of the evidence or information on a trial's outcome"), the United States Attorney's Manual, at §9-5.001[A] & [B], focuses the prosecutorial disclosure obligation instead on the concept of "materiality," advising that "ordinarily[] evidence that would not be admissible at trial need not be disclosed"); *see also Cone v. Bell*, 556 U.S. 449, 470 n.15 (2009).

In addition, the government further misunderstands *Brady* material by claiming that Moalin's motive, discussed in the FIG, is not relevant in this case because "motive is not an element of any offense charged in the indictment." (CR 108, Gov. Sup. Opp., at 14.) While exculpatory material need not negate an element of the offense in order to qualify as *Brady* material, *see Brady*, 373 U.S. at 87 (requiring the production of all *favorable* material relevant to guilt or punishment); *Giglio v. United States*, 405 U.S. 150, 154 (1972) (requiring the production of information that may be used for impeachment); and *Kyles v. Whitley*, 514 U.S. at 420 (prosecution must disclose evidence that would allow "the defense to attack the thoroughness and even the good faith of the investigation"), here Moalin's motive in sending money to Somalia is inextricably tied to his intent, which is of course an element of the charged offenses (and any conspiracy charge). If Moalin's motive in sending money to Somalia was not to aid al-Shabaab, a jury could reasonably infer that he did not intend to provide material support to al-Shabaab, or engage in any conspiracy to kill persons overseas.

Also, if, as the FIG Assessment concluded, Moalin's motivation was to aid Ayrow *not* in the context of Ayrow's al-Shabaab affiliation, but rather in the context of Ayrow's clan leadership position, that would not constitute a provision of material support to al-Shabaab in violation of §2339B. *See United States v. Paracha*, not

reported in ___ F.Supp.2d ___, 2006 WL 12768, at *25 (S.D.N.Y. 2006) (trial court ruling it would instruct jury [and did] that "the government must prove that in providing material support or resources, [the defendant] did so knowing *that the material support or resources could or would be utilized to further the activities of the al Qaeda entity and not just the personal interests of al Qaeda's individual members*") (emphasis added). *See also id*. at *13, *24.

Moreover, the government's contention that it need not provide any information or material beyond what is contained in the FIG Assessment – which itself was provided in redacted form – is erroneous. Merely alerting the defense that exculpatory information or material exists, without providing any detail that could enable the defense to use such information at trial, does *not* satisfy the government's obligations under *Brady*. *See, e.g., Carriger v. Stewart*, 132 F.3d at 480 (*Brady* violation when prosecution disclosed the witnesses' prior convictions but did not provide a RAP sheet or other supporting documents); *see also United States v. Acosta*, 357 F. Supp.2d 1228, 1243 (D. Nev. 2005) (while "[r]ough interview notes of federal agents ordinarily need not be disclosed pursuant to the Jencks Act, but must be preserved[,]" they "'must be disclosed pursuant to *Brady* if they contain material and exculpatory information'") (citations and quotations omitted.)

For instance, the government could not simply inform the defense that there

existed an eyewitness who exonerated the defendant without disclosing that eyewitness' identity. Nor could the government notify the defense that a letter exculpating the defendant existed without producing the letter itself. Here, the government, in order to satisfy its *Brady* obligations, was required to provide the underlying sources, details, and documents that formed the foundation and basis for the FIG's exculpatory statements and conclusions.

Also, the potentially classified nature of the material underlying the FIG, and the collection and cross-referencing of Moalin's telephone metadata, creates another obstacle that the courts have recognized lowers the threshold for a showing that information or evidence is material for purposes of *Brady* analysis.

For example, as the Fourth Circuit has recognized in a closely analogous context – discerning what exculpatory evidence a witness solely within the government's control, and to whom the defense was denied access on national security grounds (and whom the government initially refused even to acknowledge was in U.S. custody), might possess – when a defendant is deprived of such access, the burden to be specific with respect to the material in question must be relaxed accordingly. *See United States v. Moussaoui*, 382 F.3d 453, 472 (4th Cir. 2004) (citing *United States v. Valenzuela-Bernal*, 458 U.S. 858, 870-71, 873 (1982)).[52]

[52] Nor would the classified status of any such exculpatory information render it off limits to the defense. In fact, the law is to the contrary. As the Seventh

As this Court instructed in *United States v. Van Brandy,* 726 F.2d 548 (9th Cir.1984), while the government's failure to disclose exculpatory information "must raise a reasonable possibility that it materially affected the verdict before it becomes significant[,]" when "doubt exists as to the usefulness of evidence, [the government] should resolve such doubts in favor of full disclosure. *Id*. at 552 (citations omitted). *See also Acosta*, 357 F. Supp.2d at 1233.

Circuit noted in *United States v. Dumeisi*, 424 F.3d 566 (7th Cir. 2005), the Classified Information Procedure Act's (18 U.S.C. App. III) fundamental purpose is to "protect and restrict the discovery of classified information in a way that does not impair the defendant's right to a fair trial." *Id*. at 578, quoting *United States v. O'Hara*, 301 F.3d 563, 569 (7th Cir. 2002); *see generally*, *United States v. Moussouai*, 365 F.3d 292 (4th Cir. 2004), *reh'g granted*, 382 F.3d 453 (4th Cir. 2004); *United States v. Cardoen*, 898 F. Supp. 1563, 1571 (S.D. Fla. 1995); *United States v. Anderson*, 872 F.2d 1508, 1519 (11th Cir. 1989); *United States v. Abu Marzook*, 412 F. Supp. 2d 913, 918 (N.D. Ill. 2006); *United States v. Paracha*, No. 03 CR. 1197(SHS), 2006 WL 12768, at *10 (S.D.N.Y. Jan. 3, 2006); *United States v. Poindexter*, 698 F. Supp. 316, 320 (D.D.C. 1988).

Indeed, explicit in CIPA's legislative history is the admonition that "the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without this Act." S. Rep. No. 96-823, at 9 (1980), *as reprinted in* 1980 U.S.C.C.A.N. 4302; *see also Poindexter*, 698 F. Supp. at 320.

Consequently, as the Fourth Circuit pointed out in *United States v. Fernandez*, 913 F.2d 148 (4th Cir. 1990), "[a]lthough CIPA contemplates that the use of classified information be streamlined, courts must not be remiss in protecting a defendant's right to a full and meaningful presentation of his claim to innocence." *Id*. at 154. Consistent with that mandate, CIPA also does not diminish the government's obligation to provide exculpatory material to the defendant in compliance with *Brady*. *See also United States v. Moussaoui*, No. CR. 01-455-A, 2003 WL 21263699, at *4 (E.D. Va. Mar. 10, 2003) (holding that *Brady* principles apply in the CIPA context, including information negating guilt as well as that affecting a potential sentence).

Here, the government did not adhere to that direction from this Court. It is clear from the FBI's 2011 FIG Assessment, from the FBI's 2008 personality profile of Moalin, and the post-trial revelations regarding the genesis of the 2007 investigation of Moalin, that tangible *Brady* material exists, but which the government has repeatedly refused to produce in violation of its continuing constitutional obligation to do so.

In 2013, the year this case was tried, and the year the government subsequently disclosed its collection, aggregation, retention, and use of Moalin's telephone metadata, as well as the prior investigation of Moalin that did not produce any evidence connecting him to terrorist activity, Judge Kozinski, in dissenting from the denial of a petition for rehearing, declared that "[t]here is an epidemic of *Brady* violations abroad in the land[,] and "[o]nly judges can put a stop to it." *United States v. Olsen*, 737 F.3d 625 (9th Cir. 2013), *denying reh'g* (Kozinski, J., dissenting); *see also id*. at *6 ("*Brady* violations have reached epidemic proportions in recent years, and the federal and state reporters bear testament to this unsettling trend").

As Judge Kozinski explained, "[a] robust and rigorously enforced *Brady* rule is imperative because all the incentives prosecutors confront encourage them not to discover or disclose exculpatory evidence." *Id*. at *5. Also, as Judge Kozinski recognized, "[d]ue to the nature of a *Brady* violation, it's highly unlikely wrongdoing

will ever come to light in the first place." *Id*.

In turn, that practical reality "creates a serious moral hazard for those prosecutors who are more interested in winning a conviction than serving justice." *Id*. Also, as Judge Kozinski pointed out "[i]n the rare event that the suppressed evidence does surface, the consequences usually leave the prosecution no worse than had it complied with *Brady* from the outset[,]" because, if ultimately the previously undisclosed information is deemed material, and the conviction is vacated, "the prosecution gets a do-over, making it no worse off than if it had disclosed the evidence in the first place." *Id*.[53]

[53] In his preface to Georgetown Law Center's 2015 Annual Review of Criminal Procedure, Judge Kozinski wrote that among the dozen myths of criminal justice was that "[p]rosecutors play fair[,]" elaborating that:

> the Supreme Court has told us in no uncertain terms that a prosecutor's duty is to do justice, not merely to obtain a conviction.[] It has also laid down some specific rules about how prosecutors, and the people who work for them, must behave – principal among them that the prosecution turn over to the defense exculpatory evidence in the possession of the prosecution and the police.[] There is reason to doubt that prosecutors comply with these obligations fully. The U.S. Justice Department, for example, takes the position that exculpatory evidence must be produced only if it is material.[] This puts prosecutors in the position of deciding whether tidbits that could be helpful to the defense are significant enough that a reviewing court will find it to be material, which runs contrary to the philosophy of the *Brady/Giglio* line of cases and increases the risk that highly exculpatory evidence will be suppressed. Beyond that, we have what I have described elsewhere as an "epidemic of *Brady* violations abroad in the land,"[] a phrase that has caused much controversy but brought about little change in the way prosecutors operate in the United States.[]

In addition, Judge Kozinski noted that the detriment is not only to the particular defendant who was denied the use of exculpatory information at trial, as non-disclosure of exculpatory information "erodes the public's trust in our justice system, and chips away at the foundational premises of the rule of law." *Id*. at *7. Moreover, "[w]hen such transgressions are acknowledged yet forgiven by the courts, we endorse and invite their repetition." *Id*. at *7.

As a result, in prescribing a solution, Judge Kozinski urged the courts to "send prosecutors a clear message: Betray *Brady,* give short shrift to *Giglio,* and you will lose your ill-gotten conviction." *Id*. at *8.

E. The Government's Failure to Provide Notice of the Collection of Moalin's Bulk Telephone Metadata Denied Appellants of Due Process.

The government's failure to disclose the bulk collection, retention, aggregation, and use of Moalin's telephone metadata also deprived defendants of *notice*, a critical element in any criminal prosecution, and a hallmark of Due Process, and of "integrity and fairness" in criminal trials. *See, e.g.*, *Lambert v. California*, 355 U.S. at 228 ("[e]ngrained in our concept of due process is the requirement of notice. Notice is sometimes essential so that the citizen has the chance to defend charges"); *United*

Hon. Alex Kozinski, Preface, "Criminal Law 2.0," 44 Geo. L.J. Ann. Rev. Crim. Proc. (2015), at viii-ix (footnotes omitted).

States v. Gomez, 191 F.3d at 1220 ("'[t]he central concern of the Confrontation Clause is to ensure the reliability of the evidence against a criminal defendant by subjecting it to rigorous testing in the context of an adversary proceeding before the trier of fact'") (quoting *Lilly v. Virginia*, 527 U.S. 116 (1999) (plurality op.)).

Nor is the government's non-disclosure in this case unique. In fact, as previously set forth, the government's withholding of notice of electronic surveillance is now commonplace. Particularly in light of the rash of startling surveillance-related disclosures made during the past several years – which have all occurred *after* defendants' conviction herein, and principally have not been in context of notice to defendants in criminal prosecutions, but rather by whistleblowers seeking to shed light on secret government practices – notice of the government's reliance on surveillance techniques is essential to guaranteeing due process.

Without notice of those various techniques before or during trial, Moalin could not challenge whether the government's evidence was, in fact, lawfully obtained, or whether government surveillance conducted without a warrant and without probable cause violated the defendants' rights. Notice of surreptitious electronic surveillance is routinely required in criminal cases. Courts confronted this question with the advent of wiretapping decades ago and concluded that the government could not criminally prosecute an individual while keeping the sources of its evidence secret.

Instead, defendants are entitled to know how the government monitored their communications and activities, and then to test – in an adversarial proceeding – whether the government's evidence has been derived from that surveillance. *See, e.g.*, *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972); *Alderman v. United States*, 394 U.S. 165 (1969); *see also Gelbard v. United States*, 408 U.S. 41 (1972).

Yet the government has sought to carve out an exception to this due process requirement by routinely failing to provide notice of its surveillance activities to courts and criminal defendants in cases like this one – thereby avoiding judicial review. The Constitution does not allow this evasion and perversion of the adversary system. Indeed, the result in *Clapper*, discussed previously, demonstrates the effect of casting sunlight on these clandestine surveillance programs, and permitting the courts to intervene to enforce statutory limits and vindicate constitutional protections.

1. The Government Failed to Provide Appellants with the Notice Required Pursuant to Various Statutory Authorities

Although the vast majority of the government's evidence at trial consisted of interceptions, authorized under FISA, of Moalin's communications on his cellular telephone, the record in this case leaves little doubt that the government's surveillance of Moalin extended far beyond ordinary FISA collection. However, the

government failed to give defendants, or their counsel, all of whom possessed security clearance enabling them to review the classified material that was produced,[54] any notice of any other types of surveillance that the record indicates was performed during the investigation of this case (or even the precise type of FISA authorization employed.)

As discussed above, defendants found out only *after* trial, through public statements by government officials, that the bulk telephone metadata program played an indispensable role in the investigation and prosecution of this case. Knowledge of that information before and during trial would have assisted the defense immeasurably, enabling it to seek further information concerning the role of the program in his case and to make arguments before the post-trial motion stage about the impact of the NSA bulk telephone metadata program's collection on the sufficiency and validity of the remainder of the government's evidence in this case, including its FISA applications. (CR 345-1 at 24 and n.14.)

The existence of additional electronic surveillance conducted pursuant to still-unknown authorities was exposed in the January 24, 2008, email (hereinafter the "Another Agency Email") from FBI Special Agent Michael C. Kaiser to the government's Somali linguist, Liban Abdirahman. (CR 361 at 17; *see also* CR CR

[54] Certain classified information, in the form of a summary, was reduced through the CIPA process to a Stipulation. (12RT 1732-1733.)

370, Sent. Memo Moalin, at 32-33) ("[w]e just heard from another agency that Ayrow tried to call Basaaly today, but the call didn't go through").

The Another Agency Email makes clear that, as of January 2008, "another agency" was likely monitoring Moalin on an ongoing basis *at the same time* Moalin was subject to FISA electronic surveillance by the FBI. Moreover, the Another Agency Email demonstrates that the products of the surveillance conducted by the "[]other agency" were "used" against Moalin, as Kaiser issued investigative instructions to Abdirahman as a result of the other agency's interception. (CR 370, Sent. Memo Moalin, at 32-33) ("[i]f you see anything today, can you give us a shout? We're extremely interested in getting real-time info (location/new #'s) on Ayrow").[55]

The Another Agency Email raises a host of issues that, if it had been produced in timely fashion, and not within a volume of 3500 material two days prior to the commencement of trial,[56] defense counsel would have been permitted to explore through the adversary process. Those issues, at a minimum, include: (1) how, and to what degree of confidence, the government had decided Ayrow was the person trying

---

55 Of course, the Another Agency Email does not indicate at all in what *other* ways the other agency's surveillance contributed to the investigation, and/or what evidence was derived therefrom.

56 *See, e.g., United States v. Gil*, 297 F.3d 93 (2d Cir. 2002) (*Brady* material – a memorandum by a witness supporting the defendant's defense – buried within a box of 3500 material did not constitute timely production).

to reach Moalin; (2) whether the government intercepted or monitored Moalin's communications under the FISA Amendments Act (hereinafter "FAA") or Executive Order 12,333;[57] (3) whether any FAA or E.O. 12,333 interceptions or monitoring referred to in the Another Agency Email contributed in any way to the government's initial application for FISA surveillance of Moalin; (4) whether any FAA or E.O. 12,333 interceptions or monitoring referred to in the Another Agency Email, or occurring beforehand or afterward, contributed to any of the government's applications to extend FISA surveillance of Moalin beyond its initial term; (5) whether any FAA or E.O. 12,333 interceptions or monitoring referred to in the Another Agency Email, or occurring beforehand or afterward, contributed in any way to any government applications to conduct FISA-authorized physical searches related to the investigation of Moalin; (6) whether any FAA or E.O. 12,333 interceptions or monitoring referred to in the Another Agency Email, or occurring beforehand or afterward, contributed in any way to the identification, collection, or development of any evidence in the case, including questions asked of witnesses and instructions provided to investigators or other persons working for the government during the

57 Executive Order 12,333, 46 Fed. Reg. 59941 (Dec. 4, 1981), governs the electronic surveillance of U.S. persons overseas, but does not require a warrant, any application to the FISC, or any other court approval or review.

course of the investigation.[58]

The failure of the government to give notice of any surveillance of Moalin other than the traditional FISA intercepts prevented the defense from pursuing important factual and legal arguments that should have been available to them before and during trial.

2. Due Process and Federal Statutes Require the Government to Provide Notice of Surveillance Techniques From Which its Investigation and Evidence Were Derived in Order to permit the Defendants to Challenge Their Legality.

The defense was entitled to notice of the surveillance techniques that contributed to the government's investigation to permit them to challenge the legality of the surveillance and the admissibility of the evidence generated thereby or derived therefrom. The government cannot preempt the right to seek suppression by withholding notice based on its unilateral conclusion that its methods were lawful.

---

[58] In his pretrial motion to suppress, defendants challenged any interceptions pursuant to the FAA, 50 U.S.C. § 1881a, and requested notice of any information in the government's traditional FISA applications was the product of FAA surveillance. (CR 92 at 17–18; *see also* CR 345-1 at 5.) Because the surveillance of Moalin under FISA – from late 2007 to December 2008 – straddled the date of the enactment of the FAA in June 2008, it was unknown to Moalin at the time of his pretrial motion (and remains unknown) whether any electronic surveillance of him was conducted under the authority of the FAA. Appellants noted previously, in their pretrial motions, defendants also sought disclosure of the underlying FISA applications and supporting materials under 50 U.S.C. § 1806(f) & (g).

Rather, defendants were entitled to have a *court* – not the government – decide issues implicating their basic constitutional rights. Those questions include (1) whether the government's surveillance violated the Fourth Amendment or other legal protections; and (2) whether the government's evidence is in fact "derived" from such surveillance and therefore subject to suppression. *See, e.g.*, *Keith*, 407 U.S. 297; *Alderman*, 394 U.S. 165.

In practical as well as technical terms, the only way to effectuate a criminal defendant's right to suppress illegally acquired evidence is through notice of the means utilized to engage in such surveillance. The suppression right becomes especially important when the government adopts new and intrusive surveillance techniques that are insulated from public (and sometimes even Congressional) knowledge and debate. By now, it is clear that the government routinely uses legally untested surveillance methods in aid of investigations like the one it pursued here without disclosure and it often seeks to conceal those methods in order to avoid genuine court review.[59]

---

[59] *See* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times, Oct. 16, 2013, http://nyti.ms/1r7mbDy (hereinafter "*Secret Wiretaps*") (describing government's continuing efforts to avoid giving notice of E.O. 12333 surveillance); *id.* (describing government's five-year effort to avoid giving notice of FAA surveillance); John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, http://reut.rs/1h07Hkl (describing government's use of "parallel construction" to conceal reliance on information obtained from intelligence agencies).

However, due process rights grounded in the Fourth and Fifth Amendments entitle defendants to challenge the legality of these surveillance techniques and to seek suppression of the resulting evidence. *See Wong Sun v. United States*, 371 U.S. at 486-88 (describing "fruit of the poisonous tree" doctrine); *Murray v. United States*, 487 U.S. at 536-37 (describing right to seek suppression of evidence "derived" from an unlawful search).

The exercise of the suppression right depends entirely on notice. Thus, courts have long found notice to be a constitutionally required element of surreptitious searches like wiretaps and sneak-and-peak entries. *See Berger v. New York*, 388 U.S. 41, 60 (1967) (state wiretapping statute unconstitutional because, *inter alia*, it had "no requirement for notice as do conventional warrants"); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (sneak-and-peak warrant constitutionally defective for its failure to provide explicitly for notice within a reasonable time); *United States v. Dalia*, 441 U.S. 238, 247–48 (1979) (Title III provides "a *constitutionally adequate substitute for advance notice* by requiring that once the surveillance operation is completed the authorizing judge must cause notice to be served on those subjected to surveillance") (emphasis added); *see also Gelbard v. United States*, 408 U.S. 41 (1972) (grand jury witness had right to know whether questions were based on warrantless electronic surveillance).

In fact, Congress has responded to these rulings by incorporating express notice provisions into many surveillance statutes. *See, e.g.*, 18 U.S.C. §2518(8)(d) (Title III); S. Rep. No. 1097, at 2194 (1968) (explaining the inclusion of a notice requirement in Title III's wiretapping provisions, and citing *Berger*); *see also* 50 U.S.C. §1806(c) (FISA electronic surveillance); *id.* §1825(d) (FISA physical search); §1842(c) (FISA pen register); *cf.* Fed. R. Crim. P. 41(f) (requiring notice).

As the cases above establish, the courts have long had to confront the government's use of new technologies to carry out surreptitious searches. The use of secret wiretapping and electronic recording devices in criminal investigations posed similarly novel legal problems during the previous century. The courts that addressed the legality of these methods – and promulgated the rules governing their use – were able to do so only because the defendants received notice of that surveillance.

For instance, in *Keith*, the government responded to the defendant's motion to compel the disclosure of electronic surveillance information in a national-security prosecution by publicly acknowledging that investigators had overheard the defendant's conversations using wiretaps. 407 U.S. at 299-300.

In *Kyllo v. United States*, 533 U.S. 27 (2001), the defendant was provided notice that the government's search warrant application relied on evidence gathered using thermal-imaging technology. *Id*. at 29-30. Likewise, in *United States v. Jones*,

132 S. Ct. 945 (2012), the defendant received notice of the government's use of GPS tracking in order to record his movements. 132 S. Ct. at 948. All of these watershed Fourth Amendment decisions would have been impossible if the defendants had not received notice of the government's secret searches and seizures.

Here, for those reasons, the district court should have ensured that the defense received sufficient notice of *any* surveillance of defendants' communications or activities – not just surveillance under FISA generically – to allow them to press their claims fairly. Yet the record is manifest that the government has failed to do so in this case.

As has been demonstrated in this case, the government appears to believe that it is not obligated to provide notice when it relies on the NSA's bulk collection of call records in criminal investigations. But NSA's bulk telephone metadata program plainly presents novel questions of a constitutional dimension, as well as of statutory interpretation, and two courts have already held the program unlawful. *See Clapper*, 785 F.3d 787; *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded on other grounds, Obama v. Klayman*, 2015 U.S. App. LEXIS 15189 (D.C. Cir., Aug. 28, 2015).[60]

[60] The government apparently believes that it is not obligated to provide notice *any time* its evidence is derived from E.O. 12,333 surveillance. *See* Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. Times, Aug. 13, 2014, http://nyti.ms/1wPw6l0 (hereinafter "Savage 12,333

It is not the government's prerogative to conclude secretly and unilaterally that its surveillance is legal, but withhold notice from criminal defendants on that convenient and self-serving basis. Otherwise the entire purpose of transparent and adversary proceedings would be nullified. Due process entitles the defendants to test, on the facts of this case, whether the government's evidence should be suppressed as the fruit of unlawful surveillance.

As the courts have long instructed, due process does not leave these questions to the government's sole judgment and discretion. *See Alderman*, 394 U.S.at 168 (recounting, in wiretapping challenge, Supreme Court's refusal "to accept the *ex parte* determination of relevance by the Department of Justice in lieu of adversary proceedings in the District Court"); *Kolod v. United States*, 390 U.S. 136, 136-37 (1968) (prior proceedings); *cf., e.g., United States v. Eastman*, 465 F.2d 1057, 1062-63 & n.13 (3d Cir. 1972) (concluding that Title III's statutory notice provision was "intended to provide the defendant whose telephone has been subject to wiretap an opportunity to test the validity of the wiretapping authorization").

It would make little sense if the government could pre-determine, and therefore preclude as part of its notice analysis, difficult or novel legal questions that a defendant would properly be capable of raising with the Court – if only he knew of

Article") (describing the government's view that "defendants have no right to know" if investigators derived evidence from an E.O. 12,333 intercept).

their existence in his particular case.

In this context, the government's definition of evidence "derived" from electronic surveillance is especially opaque and problematic – yet notice in many cases turns on the definition of that term. According to reports, the government has long held a "narrow understanding of what 'derived from' means in terms of when it must disclose specifics to defendants" in the context of foreign-intelligence surveillance. *See Secret Wiretaps*.

Moreover, the government has never publicly described that "narrow understanding" – either before or after its notice policies began to draw scrutiny during the past several years, thereby effectively foreclosing review of it by the judiciary, the independent branch of government tasked with deciding such issues. Yet the consequences are significant. If the government is defining "derived" evidence more narrowly than the Constitution allows,[61] and withholding notice on that basis, then it is concealing the underlying sources of its evidence, and thereby insulating them from judicial review.[62]

---

61 *See, e.g.*, *Murray v. United States*, 487 U.S. at 536-37 (prohibiting "the introduction of derivative evidence, both tangible and testimonial, that is the product of the [unlawful search], or that is otherwise acquired as an indirect result of the unlawful search, up to the point at which the connection with the unlawful search becomes 'so attenuated as to dissipate the taint'").

62 Similarly, when the government engages in "parallel construction" – in order to conceal from the defense, the courts, and even, in some instances,

Nor is the mere invocation of "national security" availing. The Supreme Court has repeatedly made clear that when the government chooses institute a criminal prosecution against an individual, it may not keep secret the sources of its evidence. For instance, more than fifty years ago, in a context that at the time was groundbreaking but is now recognized as an essential element of a fair trial (and augured passage of 18 U.S.C. §3500) the Court made clear that

> the Government can invoke its evidentiary privileges only at the price of letting the defendant go free. The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense.

Jencks v. United States, 353 U.S. 657, 670-71 (1957) (quotation omitted).

The government may not have it both ways – its secrecy and its prosecution – when an individual's liberty is at stake. Indeed, due process requires not only notice to a defendant, but it may also mandate disclosure of underlying surveillance applications or intercepts. In *Keith*, for instance, the Supreme Court compelled the government to produce records of wiretapped conversations in a national security case, even as the government threatened to abandon the prosecution if required to

---

prosecutors themselves – the nature of its underlying investigation, that constitutes a refusal to afford the notice of "derived" evidence that due process requires. *See, e.g.*, John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, Reuters, Aug. 5, 2013, available at http://reut.rs/1h07Hkl.

disclose them. *See* 407 U.S. at 318-24, *aff'g* 444 F.2d 651, 655 (6th Cir. 1971) (discussing the government's assertions). *See also* 50 U.S.C. §§1806(f) & (g).

The Court did not blink – it ordered disclosure. *See id.* at 324. The government is bound by that same choice here, in which it has relied on undisclosed surveillance programs in the conduct of its investigation. Accordingly, the government's failure to provide notice of the surveillance techniques that contributed to its investigation in this case violated defendants' constitutional right to Due Process.

As the Supreme Court recognized in *Alderman*, "[i]n our adversary system, . . . the determination of what may be useful to the defense can properly and effectively be made only by an advocate." 394 U.S. at 184; *see Franks v. Delaware*, 438 U.S. 154, 169 (1978). Here, though, as the district court itself acknowledged (even as it denied defendants' motions to gain access to crucial materials and evidence in this case, *see* CR 388 at 16-17; ER 85-86), the prosecution of Moalin proceeded in a manner "inconsistent with the adversary process." (CR 388 at 16.)

Key evidence relating to the core of the government's case was withheld from the defense, impairing both legal arguments against the introduction of evidence at trial as well as factual arguments that could have fatally undercut the government's theory at trial. Below, the district court concluded that, having "ordered the Government on several occasions . . . to comply with its obligations under *Brady*,"

and after a "careful review of all materials provided by the Government under FISA and CIPA, as well as the myriad of intercepted communications provided to the defense, the court has no reason to suspect or speculate that the Government may have faltered in its *Brady* obligations." (CR 388; ER 86.)

Yet, as subsequent events and disclosures have proven, the district court's confidence in the government's fidelity to its *Brady* obligations was misplaced. Indeed, "speculation" is not necessary; by the admission of senior government officials themselves, the government withheld from the defense crucial material and information that meets the *Brady* standard.

Thus, in denying security-cleared defense counsel notice of the surveillance techniques employed (which, even if classified, could have been seamlessly provided under CIPA), as well as other important exculpatory information to which the defense was entitled, thereby permitting the government to evade its *Brady* obligations, the district court's decisions denied defendants Due Process.

IV.

THE DISTRICT COURT WRONGLY DENIED APPELLANTS ACCESS TO EXCULPATORY EVIDENCE WHILE ALLOWING IN IRRELEVANT AND HIGHLY PREJUDICIAL EVIDENCE; THIS COURT SHOULD REVERSE

The Appellants in this case are living in San Diego and sending money to

Somalia. Their defense was that they did not intend to support a terrorist organization in its efforts to topple a legitimate government. They were sending money back to fellow clan members who were facing an invasion by an occupying power. To that end, Appellants wanted to adduce that they held beliefs which were antithetical to the Islamist fundamentalist group that would become al-Shabaab. Moalin's intended defense was that if the jury considered what he did in 2009 which eventually got him put on a al-Shabaab assassination list, the jury would know that Moalin never intended to support the terrorist incantation of al-Shabaab. And if Moalin did not support al-Shabaab referenced in the indictment, neither did his codefendants.

A. Violations of Appellants' Right to Present Their Trial Defense

1. Exclusion of Exculpatory Evidence that Appellant's Opposed al-Shabaab

Appellants sought to introduce testimony that they held beliefs antithetical to al-Shabaab which included promoting peace and advancing the rights of women and the organization of a conference in 2009 to oppose al-Shabaab. (10RT 1441.) The district court excluded this testimony as being minimally probative. (10 RT 1430.) The district court's rationale, as adopted from the government's objection, (10RT 1428), was that acts undertaken after the time period described in the indictment were not probative of Appellants' intentions during the time-frame of the indictment.

The rationale for excluding Appellant's post-indictment period acts, however, ignores consequential facts. Being a supporter or part of al-Shabaab means having deeply-seeded fundamentalist beliefs. The evidence that Appellants sought to introduce – that Appellants promoted reconciliation, the rights of women, and the education of children – are the sort of things that get one targeted for assassination by al-Shabaab and, indeed, that is what happened to Appellant Moalin. (10RT 1432.)

Federal Rule of Evidence 404(b) does not distinguish between prior and subsequent acts. *United States v. Bibo-Rodriguez*, 922 F.2d 1398, 1400 (9th Cir. 1991) ("By its very terms, 404(b) does not distinguish between 'prior' and 'subsequent' acts.") As this Court explained in *United States v. McDonald*, 576 F.2d 1350, 1356 (9th Cir. 1978), subsequent acts can be relevant to determining intent. *Cf. United States v. Whaley*, 786 F.2d 1229, 1232 (4th Cir. 1986) ("Subsequent conduct may be highly probative of prior intent.")

Here the subsequent conduct is some of the most probative evidence imaginable. The government's charges were that Appellants supported this fundamentalist, hyper-religious organization that whose members would literally blow themselves up to further cause. (4RT 662-63.) Being a supporter or member of al-Shabaab means subscribing to a particularly virulent form of Islam and the fact that these Appellants undertook actions completely at odds with the aims of al-Shabaab

are evidence that they never actually supported that entity.

Moalin was an active supporter of women and peace movements. (9RT 1394.) Both of these activities were punishable by death for al-Shabaab the terrorist organization. Moalin wanted to introduce this evidence for the purpose of showing that he had obvious ideological differences with al-Shabaab which make much less likely that he would support terrorist organization al-Shabaab.

Prejudice will be addressed below.

2. The District Court Erred in Denying Appellants' Motion for Safe Passage and by Disallowing the Videotaped Deposition of Farah Shidane.

The magnitude of the Fifth and Sixth Amendment violations and the prejudice flowing from the district court's denial of a videotaped deposition of Farah Shidane is best understood by examining the history and rulings on defense motions for safe passage which, when denied, was followed by the joint motion for a videotaped deposition of Shidane.

a. Motion for Safe Passage

On July 20, 2012, Appellants moved to take eight Rule 15 depositions. (CR 154) The government opposed the motion and on August 22, 2012, the district court denied the motion without prejudice both on timeliness grounds and because it found defendants had failed to establish extraordinary circumstances warranting Rule 15

depositions. The matter was referred to the magistrate court to act as a special master for purposes of the issue of Rule 15 depositions. (CR 181)

On October 26, 2013, the defense moved for safe passage regarding all eight witnesses it sought to depose. (CR 213) Although the government had assured counsel it would provide safe passage, it refused to put the assurance in a letter (CR 224-1) and ultimately opposed the motion, stating Shidane was unindicted co-conspirator # 1 in the Indictment. On October 29, 2012, the magistrate court denied safe passage. (CR 216.)

The defendants jointly moved for the district court to reconsider the magistrate judge's order denying safe passage for Farah Shidane. Attached to the motion for reconsideration was an e-mail from John Kline, counsel for Shidane, stating he (Shidane) would not come to Djbouti for deposition because the United States was unwilling to guarantee him safe passage. (CR 220.) The defense represented that Shidane, who was a citizen of Djbouti and currently resided in Somalia, would provide exculpatory testimony at a Rule 15 deposition. He would testify that he was part of a local administration of the Galgaguud region and actively fought against al-Shabaab. He would testify that the money received from the defendants was used for humanitarian purposes. The defense argued the government was contractually obligated to issue safe passage to and from the Djbouti depositions and by analogy

to compelled and judicial immunity cases, denial of safe passage was violative of the Due Process Clause of the Fifth Amendment as well as the Compulsory Process Clause of the Sixth Amendment. The government opposed the motion.

On November 8, 2012, the district court denied the defense objections to the magistrate court's denial of safe passage for Farah Shidane. (CR 223.) The court found with respect to the first basis of the defense motion, that there was no contract with the government and that a claim based on a promissory estoppel theory ailed because the defense had failed "to establish a clear and unambiguous promise to provide the 'safe passage' of any proposed deponent from Somalia to Djbouti, any detrimental or reasonable reliance on the alleged promise, and any injury from the failure to provide 'safe passage' to Shidane." (CR 223, p. 3-4.)

Finally, the district court concluded it lacked authority to compel the executive branch to provide safe passage for a citizen of Djbouti to travel for a Rule 15 deposition between Somalia and Djbouti. (CR 223, p. 4-5.)

The Rule 15 depositions went forward in Djbouti from November 12-15, 2012. Farah Shidane did not appear for his deposition.

b. The Motion for a Video Deposition of Shidane

Upon returning from Djbouti, the defense moved for a video taped deposition of Farah Shidane in Somalia. (CR 224) The government opposed the motion. (CR

227). The district court found the motion was untimely and that principles of reliability, trustworthiness and fundamental fairness weighed against the videotaped deposition. The district court found that while the defense cited several authorities for the proposition that a video deposition comports with Confrontation Clause, *United States v. McKeeve*, 131 F.3d 1, 8-9 (1st Cir 1997); *United States v. Medjuck*, 156 F.3d 916, 920 (9th Cir. 1998), these authorities did not discuss the reliability and trustworthiness of depositions taken in countries without a functioning executive or judicial process.

In *United States v. Banki*, 2010 WL 1063452 (S.D.N.Y. March 23, 2010), the court held that although extraordinary circumstances (unavailability and materiality) had been established, video depositions proposed to be taken in Iran were denied because "without the teeth of the penalty of perjury, the oath becomes nothing more than an empty recital." The district court concluded that as in *Banki*, not only was Farah Shidane able to provide false testimony without any repercussions, the government would be deprived of the ability to "directly observe the witnesses' demeanor, body language, and interactions in order to gauge the truth of their statements. Because the defense failed to establish procedures to establish the trustworthiness and reliability of Shidane's proposed testimony, the district court denied the motion. The court concluded the defense had failed to establish that it is

in the interests of justice to take the video deposition of Shidane." (CR 228, ER 42.) In denying the motion for a video taped deposition of Shidane, the district court stated this was not a case where the defense was denied the opportunity to take Shidane's deposition, but rather he voluntarily chose not to appear for his Rule 15 deposition in Djbouti. The court further found there was no evidence to suggest the government interfered in any way and as a Djbouti citizen, Shidane did not require a visa to come to Djbouti for his deposition.

c. By Denying Safe Passage for Farah Shidane, the District Court Violated Appellants' Right to Present a Defense and to a Fair Trial

Unaddressed by the district court in its Order denying safe passage was the defendants' rights under the Fifth and Sixth Amendment for a fair trial and to present a defense which Farah Shidane would have contributed to greatly. This was particularly true since the government knew the intercepted calls on July 8 and 21, 2008 demonstrated that the monies at issue were being sent to Farah Shidane for humanitarian use.

The district court's conclusion that the defense had failed to establish that it was in the interests of justice to take the videotaped deposition of Farah Shidane failed to address the compelling offer of proof contained in the Declaration of Alice

Fontier filed in support of the Rule 15 motion. (CR 158.) The declaration set forth the history of the Galgaduud region in central Somalia and the local administration of that region from the time of the Ethiopian invasion in 20076 through the end of 2008. The local administration was divided into committees which included a development counsel, a humanitarian committee (which created the Orphan Care Center in Guriceel), and a security committee. All during this time period, the security committee was primarily responsible for maintaining security against attacks by al-Shabaab as well as the continuing invasion of Somalia and the massive slaughter of Somalis by Ethiopians. This model of local administration was successful and was copied in other regions of Somalia, eventually resulting in the formation of local or district courts called ifkahalanes which then formed the Union of Islamic Courts. It is within this backdrop that the role of Farah Shidane and his importance in the defense case had to be viewed. Shidane was a member of the Ayr clan from the Galgaduud region and a member of the local administration in that region in July 2008. He was also a prominent member of the Union of Islamic Courts and actively opposed al-Shabaab. He would testify about the history and development of the local administration in the Galgaduud region, his role in that development and his and the local population's opposition to al-Shabaab. He would also testify, because he had known Moalin for many years and because of Shidane's role as treasurer of the

development counsel, of money he received from Moalin – money used to build and maintain the Orphan Care Center as well as money to provide critical humanitarian aid during the drought. He would have testified that the money was not intended for, nor provided to, al-Shabaab. Finally, Farah Shidane would have testified to the fight against al-Shabaab, to the danger to his own life as a result of that fight, and to the resulting need for him to flee Galgaduud and live in Somaliland for several months.

The testimony of Farah Shidane would not only have supported the central defense of this case, it was a critically important pillar on which the defense rested: that monies sent to Somalia were not to support the activities of al-Shabaab, but to provide humanitarian relief to a country torn not only by drought but by war. The defendants were deprived of that defense.

In its Order denying safe passage to Farah Shidane, the district court rejected defendants' claim that the court had authority to compel the government to provide safe passage. The district court concluded that in *United States v. Puchi*, 441 F.3d 697 (9th Cir. 1971), this Court had not discussed the legal or factual circumstances warranting the issuance of safe passage, however that is not the case. This Court discussed the specific facts of the case, including the grant of safe passage and held the district court's order granting safe passage was not an abuse of discretion. The district court did, and should have exercised, authority to order safe passage for Farah

Shidane to travel from Somalia to Djbouti and back to Somalia for a Rule 15 deposition.

However by analogy to compelled use immunity legal standards, the district court had inherent authority to fashion a judicial immunity remedy to permit Farah Shidane to travel to Djibouti. In *United States v. Herman*, 589 F.2d 1191, 1204 (3rd Cir. 1978), for example, the Court held a district court has inherent authority to fashion a judicial immunity remedy ("a case might be made that the court has inherent authority to effectuate the defendant's compulsory process right by conferring a judicially fashioned immunity upon a witness whose testimony is essential to an effective defense"). In rejecting this argument, the district court in the instant case relied on this Court's holding that a defendant may compel immunity under two circumstances: where "either (a) the prosecution intentionally caused the defense witness to invoke the Fifth Amendment right against self-incrimination with the purpose of distorting the fact-finding process; or (b) the prosecution granted immunity to a government witness in order to obtain that witness's testimony, but denied immunity to a defense witness whose testimony would have directly contradicted that of the government witness, with the effect of so distorting the fact-finding process that the defendant was denied his due process right to a fundamentally fair trial." *United States v. Straub,* 538 F.3d 1147, 1162 (9th Cir.

2008). Contrary to the finding of the district court that neither prong of the *Straub* test was satisfied, there was clear indication in the record that the government had taken any action, by stating Shidane was unindicted co-conspirator #1.

d. By Denying a Videotaped Deposition of Farah Shidane, the District Court Violated Appellants' Right to Present Their Defense

The bases of the district court's denial of the defense motion for a videotaped deposition of Farah Shidane, were (1) because he chose not to appear at the time of his deposition in Djbouti, defendants were not denied the opportunity to depose Shidane; (2) the motion was not timely; and (3) principles of reliability and trustworthiness and fundamental fairness weighed against the videotaped deposition. (CR 228.)

Farah Shidane chose not to appear at his deposition in Djbouti because he was denied safe passage both by the government and the district court. As for the issue of timeliness, the motion for a videotaped deposition would have been premature until such time that Farah Shidane actually did not appear in Djbouti for his deposition. Finally, for reasons discussed more fully below, principles of reliability, trustworthiness and fundamental fairness were misapplied by the district court. Principles of fairness, guaranteed under the Fifth and Sixth Amendment to the constitution supported the taking of Shidane's deposition by video tape.

The district court's reliance on language in it's previous Order denying Rule 15 depositions is misplaced. Contrary to conclusions in the December 10, 2012 Order, nothing would prevent the government from its ability "to directly observe" Shidane's demeanor, body language and interactions in order to gauge the truth of his statements. Government attorneys were free to attend Shidane's deposition.

As the court noted in *United States v. Banki*, 2010 WL 1063452 (S.D.N.Y. March 23, 2010), courts have approved government depositions in far-away countries to be used against the defendant. *Cf. United States v. Abu Ali*, 528 F.3d 210, 239-40 (4th Cir. 2008) (finding no Sixth Amendment violation where defendant observed Rule 15 deposition as it occurred in Saudi Arabia over two-way video link, defense attorneys were present with him and at the deposition, and he could communicate with attorneys in Saudi Arabia via cell phone during breaks). The court in *Abu Ali* faced the same challenge as in the instant case concerning the oath administered in Saudi Arabia for purposes of the Rule 15 depositions. The oath used was one used in the Saudi criminal justice system and the Fourth Circuit stated, "we cannot conclude, without more, that such an oath failed to serve its intended purpose of encouraging truth through solemnity. " The oath was, in most respects, similar to the oath used in American judicial proceeding. Furthermore, the Court noted, defense counsel was able to cross-examine the Mabahith witnesses extensively and finally, the defendant,

judge, and jury were all able to observe the demeanor of the witnesses. *Id*. at 241. "Both the defendant and the judge were able to view the witnesses as they testified via two-way video link, and the jury watched a videotape of the deposition at trial." The same principles that control when the government seeks to take videotaped deposition testimony in a foreign country should apply with equal force to videotaped depositions sought by the defense, in this case of Farah Shidane.

It is true that depositions are generally disfavored in criminal cases. *United States v. Milian-Rodriguez*, 828 F.2d 679, 686 (11th Cir. 1987). The basis of depositions being disfavored is "largely because such evidence tends to diminish a defendant's Sixth Amendment confrontation rights." *United States v. McKeeve*, 131 F.3d 1, 8 (1st Cir. 1997); *see also United States v. Drogoul*, 1 F.3d 1546, 1551 (11th Cir. 1993); *United States v. Mann*, 590 F.2d 361, 365 (1st Cir. 1978). The Sixth Amendment, however, applies to the accused and says nothing of the government's right to confront witnesses. Thus, the main constitutional objection to the use of depositions is absent in this case. Moreover, the availability of modern technology as well as new and increased migration patterns "means that certain criminal activities increasingly manifest an international cachet and, because federal courts frequently lack the power to compel a foreign national's attendance at trial, Rule 15 may offer the only practicable means of procuring critical evidence. *United States v. McKeeve,*

supra, 131 F.3d at 8-9.

There is no requirement in the Federal Rules of Evidence that a judicial officer even be present at a deposition. This Court has held admissible in criminal trials videotaped depositions at which no judicial officer was present. *See, e.g., United States v. King,* 552 F.2d 833, 838-43 (9th Cir. 1976) (videotaped deposition testimony of unindicted co-conspirators imprisoned in Japan where defense counsel were present to cross-examine the deposed witnesses was held admissible). In addition the concerns of the district court in the instant case regarding the lack of a judicial officer's presence to review and rule on objections to the deposition proceedings, Fed. R. Crim. P. 15 provides for preservation of such objections by requiring that "objections to deposition testimony or evidence or parts thereof and the grounds for the objection shall be stated at the time of the taking of the deposition." Fed. R. Crim. P. 15(g). *See also Torres-Ruiz v. United States District Court,* 120 F.3d 933, 936 (9th Cir. 1997).

The testimony of Farah Shidane was necessary for a fair trial. His testimony, as outlined above and in the Declaration of Alice Fontier, was unequivocally material. *United States v. Jefferson*, 594 F. Supp.2d 655, 667 (E.D. Va. 2009). There was no issue of Shidane's unavailability. Finally, any security concerns regarding government attorneys traveling to Somalia could be eliminated by a live videotaped

deposition should government attorneys choose not to travel to Somalia; they could observe the live videotaped deposition while in the United States, Djbouti, or anywhere else they desired to be. If a defendant's participation in a Rule 15 deposition via video conference is sufficient to meet the demands of the Confrontation Clause (*see United States v. McKeeve, supra,* 131 F.3d 8-9; *United States v. Medjuck*, 156 F.3d 916, 910 (9th Cir. 1998)), certainly such a procedure would not have unduly prejudiced or inconvenienced the government in this case.

B. The District Court Erred by Overruling Defense Objections to the Highly Prejudicial and Unnecessary Presentation of the Black Hawk Down Incident

The United States is currently at war with some (but not all) Islamic Fundamentalist groups. Most famous, of course, is al-Qaeda. Everyone in this case agreed that al-Qaeda was not part of the case. (1RT 63.) The Court did, however, spend sometime in voir dire explaining how this case was not about al-Qaeda, though it might be mentioned during trial. (1RT 65.) This set the tone for the 403 violating "us versus them" narrative adduced at trial.

Over objection, the United States was allowed to adduce testimony about the "Black Hawk Down" incident in 1993 which recounted the famous incident where two Black Hawk helicopters were downed leaving United States's special forces troops isolated deep in Mogadishu. 18 soldiers and a thousand or more Somalis were

killed. (3RT 458-60.) The tragedy would become the subject of a very successful motion picture "Black Hawk Down."[63]

The district court answered Appellants' objection by saying that the Black Hawk down incident was part of the chronology. (3RT 458.) The "Black Hawk Down" incident is probably relevant to many chronologies and it is an event that happened in Somalia and between the United States and a warlord, but it bears no relevance to the charges against Appellants. "Al-Shabaab" the terrorist organization does not owe its origin to Black Hawk Down and the incident bore no relation to the charges before the Court.[64]

Under the 403 test, the district court is asked to weigh probative value of the Black Hawk down incident – unrelated to any of the charges or the story the government wanted to tell – against its possible prejudicial effects. The Black Hawk Down story is about 18 American soldiers – medal of honor winners – who got murdered and had their bodies desecrated by a Somali mob in Mogadishu. The substantial prejudice to Appellants is obvious: it reminded the jury that we had fought a war against certain Somali enemies and had lost in tragedy.

---

63 The film won two Oscars and brought in $173,000,000 at the box office. https://en.wikipedia.org/wiki/Black_Hawk_Down_(film);

64 *Cf. United States v. Waters*, 627 F.3d 345, 356 (9th Cir. 2010)(Evidence of inflammatory anarchist literature erroneously admitted because prejudicial effect substantially outweighed probative value.)

Appellants rely on *United States v. Al-Moayad*, 545 F.3d 139 (2nd Cir. 2008), in which the Second Circuit reversed material support convictions in a sting-operation case because the district court allowed in testimony about the Israeli bus bombings during trial even though it was unrelated to the charges against the defendants. Here, Black Hawk down had no relation to these Appellants and carried a risk of substantial prejudice. It ought to have been excluded.

C. Prejudice and Cumulative Error

The government's case is built upon circumstantial evidence, but it is not DNA evidence. For all of the recorded calls, there is no direct evidence of money being sent by Appellants as ear-marked for al-Shabaab the terrorist group. The situation in Somalia is fluid enough and the language labile enough that Appellants did not mean to send support to the terrorist organization. They ought to have been allowed to present their defense in full and without prejudicial and irrelevant information.

Appellants sought to introduce the testimony about the 2009 conference because it was the product of his actions and intent through the 2007-08 period of the indictment. (1431.) This was crucial evidence for Appellants' defense and its exclusion violated their right to present a defense. *See, e.g.*, *Chambers v. Mississippi*, 410 U.S. 284 (1973); *Chia v. Cambra*, 360 F.3d 997, 1003-08 (9th Cir. 2004). "In balancing the interest of a state in enforcing its evidentiary rules against the interest

of defendants in presenting relevant evidence in their defense, [the Ninth Circuit] consider[s] the so-called *Miller v. Stagner,* 757 F.2d 988, 994 (9th Cir. 1985), factors: the probative value of the evidence on the central issue; its reliability; whether it is capable of evaluation by the trier of fact; whether it is the sole evidence on the issue or merely cumulative; and whether it constitutes a major part of the attempted defense." *United States v. Stever*, 603 F.3d 747, 756 (9th Cir. 2010) (quoting *Alcala v. Woodford*, 334 F.3d 862, 877 (9th Cir. 2003).

The *Miller* factors require admission of this evidence: Appellants were accused of supporting al-Shabaab so evidence that they were fundamentally opposed to al-Shabaab directly contradicts the charge in the indictment. This evidence was not cumulative of other evidence because no other evidence directly demonstrated Appellants' opposition to al-Shabaab.

Appellants also should have been allowed to adduce Farah Shidane's testimony which would have exculpated Appellants and been "directly contradictory" to the government's evidence. *Straub* explains the impact on Appellants' right to a fair trial:

> A survey of our opinions suggests that in the majority of cases where a defendant seeks to compel immunity for a witness, that witness's testimony will not be "directly contradictory" to that of the prosecution's witness, or there will have been no distortion of the fact-finding process, and the district court may deny immunity on those bases. *See* [*United States v. Alvarez*, 358 F.3d 1194, 1216 (9th Cir. 2004)] (the testimony sought did not directly contradict statements by the government's

> witnesses); [*United States v. Duran,* 189 F.3d 1071, 1087 (9th Cir. 1999)](neither the Lord test nor the [*United States v. Westerdahl*, 945 F.2d 1083 (9th Cir. 1991)] test was even applicable); [*United States v. Baker*, 10 F.3d 1374, 1414-15 (9th Cir. 1993)] (defendant not even charged with [1162] the crime about which defense witness offered testimony); [*United States v. Brutzman*, 731 F.2d 1449, 1452 (9th Cir. 1984)] (evidence was cumulative or "not exculpatory"); [*United States v. Alessio*, 528 F.2d 1079, 1082 (9th Cir. 1976)]("The testimony sought by appellant was cumulative . . . ."). As we discuss below, this case appears to be the rare case in which the testimony was in fact directly contradictory. Furthermore, the prosecution granted immunity and other incentives to eleven of Straub's co-conspirators, while denying immunity to the one witness who had testimony that, if believed, would make the government's key witness both a perjurer and possibly the actual perpetrator of the crime. There is an unmistakable air of unfairness to a trial conducted under these circumstances, one that calls into question the fundamental fairness of Straub's trial and the meaningful protection of his due process rights.

As in *Straub*, the testimony of Farah Shidane was directly contrary to the testimony presented by the government regarding the use of funds sent through the Shidaal. The control of exculpatory evidence was impermissibly left in the hands of the government.

The exclusion of Appellant's defense evidence combined with the admission of irrelevant and highly prejudicial government evidence make this a prime case for cumulative error. *See Parle v. Runnels*, 505 F.3d 922, 927-28 (9th Cir. 2007). Alternatively, this Court could grant relief per its supervisory powers. *See, e.g.*, *United States v. Frederick*, 78 F.3d 1370, 1381 (9th Cir. 1996); *United States v. Tory,*

52 F.3d 207 (9th Cir. 1995). Furthermore, even if some of Appellants' claims are only reviewed for plain error, such errors are also considered in the cumulative error analysis. *See, e.g., United States v. Fernandez*, 388 F.3d 1199, 1256-57 (9th Cir. 2004); *United States v. Wallace*, 848 F.2d 1464, 1476 n.21 (9th Cir. 1988); *accord United States v. Al-Moayad*, 545 F.3d at 176-78.

V.

THERE WAS INSUFFICIENT EVIDENCE FOR THE JURY TO CONCLUDE THAT ISSA DOREH CONSPIRED TO PROVIDE MATERIAL SUPPORT TO TERRORISTS (COUNT 1), TO PROVIDE MATERIAL SUPPORT TO A FOREIGN TERRORIST ORGANIZATION (COUNTS 2 AND 5), AND TO LAUNDER MONEY (COUNT 3)

A. Doreh's Argument is Preserved

A the close of the government's case, counsel for all defendants moved for a judgment of acquittal. (7RT 1248.) The district court denied the motion as to each defendant on each count. (7RT 1250.)

B. The Backdrop: Famine, Drought, and the Occupation of Somalia by Ethiopia

The backdrop against which the intercepted phone calls, particularly those involving Issa Doreh, must be understood requires an understanding of the impact of the Ethiopian invasion of Somalia as well as death and displacement of hundreds of thousands of Somalis at the hands of Ethiopians as well as famine and drought that

had plagued the country.

The Republic of Somalia was formed in 1960. (3RT 449, 452.) There was a brief power vacuum after the assassination of one of the early presidents; a vacuum that was filled by a military coup and General Muhammad Siad Barre emerged as the new (military) president of Somalia. Although Barre set up the Somali Revolutionary Socialist Party, his government essentially remained a military dictatorship for 21 years. (3RT 453.) Rebellions have been common in various parts of Somalia since the late 1970's and during the 1980's, these rebel groups multiplied and became more active. (3RT 453-54.) As the Barre government became weaker, finally in1989-1990, rebel forces moved from central Somalia to Mogadishu and the uprising started in the capital at the end of December. The Barre government was eventually exiled. (3RT 454.)

Initially there was no government in January 1991, however the rebel movement entered the capital and the United Somali Congress, which had two factions, and one declared a transitional government. (3RT 343-455.) In July 1991, the transitional government received some recognition from other states, but that did not last long. (3RT 454-55.) The two wings divided and fighting began in November 1991; fighting which created a humanitarian crisis in Mogadishu as well as other parts of Somalia and which led to the death of about 30,000 people in Mogadishu

alone and the displacement of hundreds of thousands of others. (3RT 455.) This fighting, as well as drought conditions, led to famine conditions across much of southwest Somalia. (3RT 456). The United States pulled out of Somalia in April 1994 and the United Nations pulled out its forces one year later. (3RT 461.) In 1995, after the U.N. pulled out, there was no stable government in Somalia.

In 2000, efforts were made to establish a stable government in the form of a Transitional National Government. In the early 2000s, the SRRC (Somali Restoration and Reconciliation Council) was Ethiopian-backed and formed to undermine the TNG. (4RT 607.) Many of their leaders were warlords. (4RT 609.) Furthermore, Ethiopia backed militias in Somalia to limit the control that the TNG could exercise in the country. (4RT 610.) Four years later, the Transitional Federal Government (TFG) was formed. The TFG was formed in 2004 in Kenya and former military officer Colonel Abdullah Yusuf Ahmed became the president. Mogadishu was considered not only to be insecure , but actually hostile to the new government. (3RT 463.) President Yusuf called for 20,000 foreign troops, most of whom were Ethiopian. Yusuf's SRRC had been backed by the Ethiopians in th first place. His appeal for 20,000 foreign troops was widely perceived as an act of ventriloquism from Addid Ababa aimed at putting Ethiopian boots on the ground in Somalia. (4RT 613.) Ethiopia was concerned about the Islamic courts expanding outward from

Mogadishu; Ethiopia had its own regional agenda. (4RT 613.) Although not supported in its own country, the TFG was welcomed as a new interim government by the international community and representatives were accepted as official representatives of Somalia in the United Nations; humanitarian aid began to flow. (3RT 473.) The central state in Somali history has been predatory and typically a source of insecurity and fear for the Somali population. The average Somali had good reason to be cautious and skeptical of the initiative to reestablish a government. (4RT 599-600.)

By Spring 2006, the TFG was still in the Baidoa area. In June and July 2006, Mogadishu was taken over by the Union of Islamic Courts which was an umbrella organization for courts in Mogadishu and other parts of southern Somalia. Although there had been Islamic Counts practicing sharia law for some time, the number of courts grew from three or four in 1998 to over 12 in 2006. (3RT 476-77.) Each Court had a militia that functioned as a kind of police force members wore a distinctive red head cloth and carried assault weapons and rocket-propelled grenades and other light weapons. (3RT 477-478.) They drove pickup trucks or four-wheel-drive vehicles with the tops cut off and a heavy machine gun mounted on the back; these vehicles were known as "technicals." (3RT 477-478, 480-81.) Somali militias were typically lightly armed; Kalashnikov-patterned assault rifles, RPG 7 rocket-propelled grenades, PKM

machine guns, and then crew-served weapons such as 12.7 mm heavy machine guns mounted on a truck and the bigger weapons would be 23 and 37 mm antiaircraft cannons mounted on vehicles. (3RT 478.)

Arms and weapons are commonplace in Somalia; they have been for a long time. (4RT 593.) During the Barre regime, Somalia was one of the best equipped armies in Africa; armed first by the Soviets, then by the west. (4RT 593.)

According to Bryden, RPGs are not limited to al-Shabaab; everyone/militias who wants one can get it. (4RT 596.) Technicals (heavy trucks with weapons mounted) existed long before al-Shabaab; they were probably the most distinctive feature of the early 90's. Somalia does not have an air force, not even helicopters. (4RT 596.) Combat aircraft was limited to Ethiopia. (4RT 596.)

Hassan Dahir Aweys eventually emerged as a behind-the-scenes leader of the Islamic Courts Union which was seen, when it emerged in Mogadishu, as a direct challenge to the TFG. As the Courts Union expanded its territory across southern Somalia, this led to a direct confrontation and fighting broke out. In Summer 2006, the Islamic Courts Union took over Mogadishu. (3RT 484.) During the second half of 2006, peace talks between the TFG and Islamic Courts Union broke down and clashes occurred outside Baidoa, threatening the TFG and Ethiopian forces there. The Ethiopian offense was very fast and the Islamic Courts were defeated in central

Somalia and in Mogadishu. (3RT 485.) As a result, the Courts went underground and emerged a couple months later as part of a broad-based and complex insurgency against the Ethiopian intervention and against the TFG which in January 2007, had been brought back to Mogadishu by the Ethiopian military. It was then that al-Shabaab emerged as its own entity. (3RT 486.)

Al-Shabaab was only one of a number of insurgency groups fighting the TFG and its master, the Ethiopians. During 2007, there was ongoing fighting between Ethiopians and TFG on one side and various insurgent groups, including the Islamists and al-Shabaab, on the other. (3RT 541.) The United States and the United Nations continued support of the TFG which was known to be corrupt and inefficient and in February 2007, the United States Security council approved deployment of African Union forces (which included Ethiopians) into Somalia. (3RT 540-42.)

It would be a mistake to continue the mis-characterization of al-Shabaab as the sole insurgency group in Somalia in 2007 and 2008. According to government witness Bryden, Somalia is characterized by complex fluid allegiances, shifting alliances, and sometimes people have more than one. There were groups other than the Alliance for the Reliberation of Somalia (ARS) and al-Shabaab fighting to overthrow the TFG. ARS engaged in its own fighting against Ethiopian and AMISON forces, (3RT 543-44.) Jabiso was another group which sometimes fought alongside

al-Shabaab and ARS to overthrow the TFG, which continued to be supported by the Ethiopians. (3RT 545-546.) In 2007, Ethiopian support included military on the ground and also aerial support. (3RT 546.)

Bryden explained, It was not simply al-Shabaab versus the TFG. He wrote, there was a "violent insurgency that involves a broad range of opposition forces motivated by clan, nationalists, and Islamic agendas." It was a "very broad based insurgency." (4RT 605.) He added that in 2007 and 2008, many different militias fought in the same areas because they had a common enemy; sometimes they cooperated and sometimes they did not. (4RT 657.)

During all of this time of political strife, droughts, including one in 2006-2008, and famine had a particularly negative impact on children's nourishment. Somalis also suffered from 1991 through 2006 and again from 2006 to 2008 and a significant number of deaths occurred from the armed conflict with Ethiopians. (4RT 577.)

The Somali diaspora tends to identify closely with events in Somalia and are among the most active Internet communities. According to government witness Matthew Bryden, the Somali diaspora has been a critical source of political and financial support for activities in Somalia, sending between $500 million and $1 billion back to their homeland every year. Links between the diaspora and Somalia itself are very active. (4RT 582.)

The Ethiopian occupation of Somalia lasted three years, from 2006 to 2009; Ethiopia began to withdraw in January 2009. (4RT 612.) Bryden wrote in October 2007 in a confidential memo to USAID "Ethiopian intervention in Somalia has triggered a persistent and escalating insurgency." (4RT 614-615.) And Somalia had degenerated into a violent and costly occupation for which the United States was, according to Bryden, widely held to be responsible. He also wrote, Ethiopia "accentuates the threat of terrorism in order to secure international, especially American, support. (4RT 614.) In both Somalia and the Ethiopian/Somali regional state, Ethiopia had installed narrowly based compliant governments that lacked local legitimacy and disenfranchised segments of the population. The main point made by Bryden was that U.S. interests included stabilization and counterterrorism but this policy was having the reverse effect in creating radicalization and instability in Somalia. (4RT 616.)

Ethiopia had had forces in Somalia at other times, however during the time of the transitional government, Somalis did not accept the Ethiopian military presence party they were an occupying military force and because they supported the TFG. Also, Ethiopia was blamed for certain civilian deaths, destruction of property; interference with local administration through support of the TFG. There was also a historic antagonism between Somalia and Ethiopia. (4RT 617.)

The scope of the problem for Somalis both in Somalia and in the diaspora was massive. In 2007, there was massive displacement because of fighting in Mogadishu. Many people had returned to Mogadishu during the rule of the Islamic courts because of the stability there. In 2007, when the Ethiopian military came, there was some initial displacement out of fear that there would be violence. When heavy fighting began in March 2007, the estimates were that between March and June, about 700,000 people left Mogadishu, many of which fled and settled along the road. Some are still there. (4RT 644-645.) Ethiopia was blamed for civilian deaths and destruction of property and interference with local administration through its support of the TFG. (4RT 617.) The peak of the hundreds of thousands of people camped along the highway going out of Mogadishu was from the end of 2007 and into 2008. (4RT 647-49.)

C. There Was Not Only Insufficient Evidence, There Was No Evidence that Issa Doreh Conspired to Provide Material Support to Terrorists (Counts 1, 2, and 5) or to Launder Money (Count 3).

Issa Doreh was charged in Count 1 of the Second Superseding Indictment with conspiracy to provide material support to terrorists in violation of 18 U.S.C. § 2339A(a); Count 2, conspiracy to provide material support to Foreign Terrorist Organization in violation of 18 U.S.C. § 2339B(a)(1); Count 3, conspiracy to launder monetary instruments in violation of 18 U.S.C. § 1956(a)(2)(A) and (h); and Count

5, providing material support to foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1) and 2. (CR 147; ER 1-12.)

As to all four counts, a conspiracy requires an agreement to engage in criminal activity, one or more overt acts taken to implement the agreement, and finally, the requisite intent to commit the substantive crime. *United States v. Sullivan*, 522 F.3d 967, 976 (9th Cir. 2008); *United States v. Penagos,* 823 F.2d .346, 348 (9th Cir. 1987). Evidence establishing a defendant's connection with the conspiracy beyond a reasonable doubt is sufficient to support the defendant's knowing participation in the conspiracy, once the existence of the conspiracy has been shown. *United States v. Hernandez*, 876 F.2d 774, 779 (9th Cir. 1989) ; *see also United States v. Candoli*, 870 F.2d 496, 511 (9th Cir. 1989); *United States v. Monroe*, 552 F.2d 860, 862 (9th Cir.1977).

Count 1 charged a conspiracy to provide material support to terrorists, [conspiracy to kill persons in a foreign country] and 2332a(b) [conspiracy to use a weapon of mass destruction outside of the United States], all in violation of § 2339A(a). The Second Superseding Indictment set forth 16 overt acts in furtherance of the conspiracy alleged in Count 1. Proof of the commission of an overt act in a § 2339A conspiracy is not required by statute. See 18 U.S.C. § 2339A; *see also United States v. Stewart*, 590 F.3d 93, 114-116 (2d Cir. 2009).

To convict Issa Doreh on Count 1, the government was obliged to prove: (1) that he entered into a conspiracy; (2) that the objective thereof was to provide material support or resources to al-Shabaab; and (3) that Doreh then knew and intended that such support or resources would be used in preparation for, or in carrying out, a separate conspiracy to murder, kidnap, or maim outside of the United States. *See* 18 U.S.C. § 2339A; *United States v. Hassan*, 742 F.3d 104 (4th Cir. 2014); *United States v. Chandia*, 514 F.3d 365, 372 (4th Cir. 2008). With respect to the first element, the government was obliged to prove a conspiracy — that is, an agreement between two or more persons to engage in illegal activity. *See United States v. Burgos,* 94 F.3d 849, 857-58 (4th Cir. 1996) (en banc). Issa Doreh's involvement in such a conspiracy would be adequately demonstrated if the evidence showed "a slight connection between [him] and the conspiracy." *See United States v. Kellam*, 568 F.3d 125, 139 (4th Cir. 2009) (internal quotation marks omitted). Furthermore, the "existence of a tacit or mutual understanding is sufficient to establish a conspiratorial agreement, and proof of such an agreement need not be direct — it may be inferred from circumstantial evidence." *Id.* No such evidence, tacit or otherwise, was presented that Issa Doreh had entered into an agreement with anyone to engage in illegal activity. His only aim was as a member of the disapora, to help protect his home from the Ethiopian invasion and to send humanitarian aid to

Somalia. The government never proved that Doreh ever supported al-Shabaab or Aden Ayrow. It should be noted here that the government admitted it did not know and could not prove that the person identified as Sheikalow (on any intercepted calls, including the 11 calls Issa Doreh participated in) was in fact Aden Ayrow.

Even if Issa Doreh was found to have supported an insurgency against Ethiopia, there was no proof that that insurgency was either al-Shabaab or a terrorist group let alone a group designated by this Country as an FTO. As to the second element of the conspiracy charged in Count 1, "material support or resources" has been is defined as "any property, tangible or intangible, or service," including "currency," "training," "expert advice or assistance," "weapons," or "personnel." 18 U.S.C. § 2339A(b)(1). The third element required the government to establish that Issa Doreh acted "with the knowledge or intent" that such material support or resources would be used to commit a specific violent crime, in this instance a violation of 18 U.S.C. § 956. *See United States v. Stewart,* 590 F.3d at 113.

The language used in Count 1 contains the essential elements of § 2339A, including: (1) an agreement; (2) to provide material support (3) with the knowledge or intent that it will be used in preparation for a violation of 18 U.S.C. § 956 (conspiring to kill persons in a foreign country) and 18 U.S.C. § 2332a(b) (conspiring to use a weapon of mass destruction outside of the United States).

The district court instructed the jury as to the knowledge requirement in the instruction concerning Count 1 and instructed jurors that "[o]ne who has no knowledge of a conspiracy but happens to act in a way which furthers some object or purpose of the conspiracy does not thereby become a conspirator. Similarly, a person does not become a conspirator merely by associating with one or more persons who are conspirators nor merely by knowing that a conspiracy exists." (13RT 1790.) Also included in that instruction was the following: "Proof that people simply met together from time to time and talked about common interests such as political views or religious beliefs or engaged in similar conduct is not enough to establish a criminal agreement. Such association or speech, standing alone, is protected by the First Amendment." (13RT 1791.)

As to Count 2, as part of the instruction on the elements, the district court instructed jurors again that a defendant 'became a member of the conspiracy knowing of its unlawful object and intending to help accomplish it." (13RT 1794; emphasis added.)

A similar instruction was given as to Count 3,namely that in order to be found guilty of conspiracy to launder monetary instruments, "the defendant became a member of the conspiracy knowing of its unlawful purpose and intending to accomplish it." (13RT 1795-1796, emphasis added).

And finally, as to Count 5, the district court again included "knowledge" in its instruction to jurors, namely "One, on or about April 23, 2008, the defendant knowingly provided material support or resources to al-Shabaab." (13RT 1798.)

Under the instructions given by the district court as to Counts 1, the government had to prove beyond a reasonable doubt for purpose of count 1 that Issa Doreh intended to commit murder and/or he intended to provide material support for a weapon of mass destruction. As to either, mere recklessness or knowledge would not satisfy the government's burden. *See United States v. Chhun,* 744 F.3d 1110, 1117 (9th Cir. 2014). When viewed in the light most favorable to the government, the evidence was insufficient to show that Issa Doreh had the requisite mens rea of intent to commit the offenses in Count 1, namely murder and/or to provide a weapon of mass destruction.

Similarly, as to Count 2 which alleged a conspiracy to provide material support to a foreign terrorist organization in violation of § 2339B. The government had to prove Doreh became a member of the conspiracy charged in Count 2 knowing of its unlawful object and intending to help accomplish it. Again, there was not only insufficient evidence, there was no evidence to support a finding that Issa Doreh knew of any unlawful object nor that he intended to accomplish an unlawful object by doing his job which was to act as a minor player in the Shidaal Express. As the

government well knows, when Basally Moalin asks Issa Doreh states on April 23, 2008 for the name of the sender, Doreh says, "Well he is not here now; he is the one who sent it, I can't log into the website; I don't have an account, I don't send money, you know." When asked who sends the money, Doreh says "Abdirizak is the person who sends the money." (Exhibit 159; 6RT 1059.)

Count 3 required that Issa Doreh knew of the unlawful purpose of a conspiracy to lauder money and intended to accomplish the unlawful purpose. Again, the evidence presented by the government was that Doreh was a clerk in the Shidaal Express; a person who had no access to the actual mechanics of money transfers. The government knew this not only on the basis of its investigation and indictment of the owner of the Shidaal Express (Abdirizak Hussein) but because of Doreh's statements on the intercepted calls.

Again, as is true in the case of Counts 1-3, a necessary element of Count 5 in the case of Doreh was that he "knowingly provided material support or resources to al-Shabaab" and there was no evidence to support such an allegation.

Contrary to the government's theory and argument at trial, evidence presented to the jury proven Issa Doreh was not only not able on his own to grant discounts or to transmit monies from San Diego to Somalia, every transaction was approved not by him but by Donnah Locsin. (4RT 761.) Additionally, during a call on April 23,

2008 (Exhibit 159; 6RT1059), Moalin asks Doreh about the name of a sender on a particular transfer and Doreh says "he" (meaning Abdirizak) is not here now and "he" is the one who sent it and that he (Doreh) can't log into the website, "I don't have an account, I don't send money, you know." (*Id*. p. 2.) Abdisalam Guled testified that money was sent to Somalia from the disapora through a hawala and that when money is sent through a hawala by a recognized charity that has an account with the hawala, normally a fee is not charged. If it is not recognized as charity, but the promise of charity sending of this money (outreach or hospital), the fee is minimized, but still charged. (12RT 1687)

Furthermore, contrary to the government's contention and argument to jurors, discounts were made by the owner, Mohamud Ahmed and his business manager, Abdirizak Hussein, not by Issa Doreh. The government knew full well that this was true as reflected in the separate indictment (Southern District of California, Case No. 13CR1514-JM, filed on April 23, 2013) in which Abdiaziz Hussein (aka Abdiaziz Hussen, aka Abdirizak) was alleged in Count 1 to be "Shidaal's manager and responsible for daily operations from 2007 until approximately November 2009."[65] Of particular interest is the fact that overt acts relating to transfers on April 23, 2008 and April 25, 2008 mirrored those in Doreh's indictment as caused by Moalin, Issa

[65] Issa Doreh asks this Court to take judicial notice of not only the Indictment in 13CR1514-JM, but also Hussein's guilty plea.

Doreh and Mohamud Mohamed, however the government alleged in 13CR1514 that these transfers were caused by Hussein. (CR 147; ER 7-8.) In fact, Issa Doreh did not have access to the money wiring equipment; he did not have an ID and password d to enter the system and he certainly was not, as argued by the government, in a position to waive fees or discounts. The government's argument at page 13RT 1974 of its rebuttal argument, that Moalin told someone named Sheikalow that Issa Doreh could waive the fee does not make it true.

The Second Superseding indictment states, in Overt Act 11, "on or about July 15, 2008, defendant Doreh caused the transfer of $2,280 from San Diego, California to Somalia." (ER 8.) The government argued the same at the time of trial. Not only did the government know that Doreh did not have the access, authority or power to transfer money to Somalia, the government also misrepresented the transfer of $2,280 as personally sent by him. That money, as the government knows well from its translation of the intercepted calls on July 8 and 21, 2008 was sent to Farah Shidane who was not affiliated with al-Shabaab, but was involved in humanitarian relief. While presenting the fact of the transactions during trial, the government concealed from jurors the actual intercepted calls which would have shown the recipient was Farah Shidane who worked to provide humanitarian relief in Somali. His efforts were completely opposed by al-Shabaab. The fact that funds were sent from the diaspora

to Somalia for humanitarian relief is evidenced in a call on February 18, 2008 presented as a defense exhibit. In that call, which is between Moalin and Sahal (who had been mentioned in the first call as the guy that runs the orphanage, Issa Doreh is introduced to Sahal as the guy that runs the orphanage. Government witness Bryden also testified to the money sent by members of the diaspora to Somalia. (3RT 440.)

In Exhibit 182, which is a call at 04:56:39 UTC on July 2, 1008, between Farah Shidane, Moalin and Mohamed Mohamud, there is a lengthy discussion of fighting, however the attack by Farah Shidane and his people were of Ethiopians. He makes clear in this conversation when he says "The situation changed and our army was forced to follow them and attack the Ethiopians from the rear. This was the first time in one year of fighting that we attacked them from behind while they were in retreat." (Exhibit 182 at p. 6-7; 6RT 1090.) If the government is correct, certainly not conceded by Doreh, that references to "the youth" was in fact a reference to al-Shabaab, the distinction between what Farah Shidane's men were doing and what "the youth" were doing is great. Farah Shidane says in that same call that "The Youth fought for three minutes and left. That resulted in some of our brothers being exposed to danger and the enemy came around and killed some of our men, like professor Aspro and others, although they fought well. Furthermore, other groups of fighters joined the fight and it continued for four hours without stop. (*Id*.) Farah Shidane says,

in response to Sheik Mohamed's question, that the Somali Islamic Liberation Organization and his (Shidane's group) are the same. (*Id*. at 4 of 7.) At no time does Shidane or anyone else say that the Somali Islamic Liberation Organization is the same as or affiliated with al-Shabaab.

With respect to the government's allegation and argument that Issa Doreh caused the transfer of $2,280 from San Diego to Somalia on July 15, 2008 (Count 1, Overt Act 11(n), there are four calls on July 8, only three of which (Exhibits 183, 184 and 185; 5RT 886, 889, 6RT 1117) were introduced into evidence by the government. Exhibit 184 is a call on July 8, 2008 from Moalin and Doreh to Mohamed Abdi Hassan Yusuf. This call clearly concerns monies collected were intended to be sent to the students of the Koran School; the people and the orphans. He continues to say that the money has been divided into three Koran schools. Hassan says he and the children don't have anything to transport the grain and no means of transportation for these books. (Exhibit 184 at p 7.)

Exhibit 185 is also a call on July 8, 2008 from Moalin to Doreh who says, when asked if he sent the money, says "I gave the money to Mohamud. I didn't send the money." (6RT 1117.) At the time of this call, Mohamud Ahmed was the owner of Shidaal Express.

The fourth call on July 8, 2008 was not played by the government. That call,

which took place at 21:10:54 UTC was from Moalin to Farah Shidane. Moalin tells Shidane that he has deposited $5,000 at Amal, using the name Dhunkaal. Shidane explains that he was part of a convoy of at least six cars, including the Ugaas and the elders, that went to visit the brothers and give them $10,000 intended for the families they had left behind.

On July 21, 2008, there is another call not played by the government. It was at 03:51:48 UTC from Moalin to Farah Shidane who says he received $1,030 at one time and $1,250 at another time. These funds are the monies the government attributes to Issa Doreh as going to terrorists when they were clearly for Farah Shidane who was neither al-Shabaab or a terrorist.

The government had no evidence to support the allegation that Issa Doreh "caused the transfer of $2,280 from San Diego, California to Somalia." In fact, in a call on July 22, 2008 at 17:25:20 between Moalin and Issa Doreh, Moalin says the transfer belonged to the children and Doreh clearly says Right, actually I was not present and the man I delegated was absent for awhile. He was not even available yesterday when they did the inquiry." (Exhibit TT-196A; 10RT 1511) As the evidence at trial clearly established, Farah Shidane was involved in humanitarian works. In fact, money from the diaspora for humanitarian work is a threat through the government's intercepted calls. As early as December 2007, there were discussions

about fund-raising for orphans, for a school called ILEYS and mention of a man by the name of Sahal who ran an orphanage.

Despite knowing that from its own translation of the calls, the government argued to the jury "What's clear is that Issa Doreh was a person of enough importance at Shidaal Express to tell the Shidaal Express people to waive the fee if that's what he wanted to have happen. That's what he told Aden Ayrow about Doreh, and I already reviewed that call in the opening close; he said yes, he's the guy that waives the fee for us. And that's when Basaaly was speaking to Aden Ayrow." (13RT 1974.)

Additionally, not only did the government never prove that the Sheikalow referenced on the calls was Aden Ayrow, there was no evidence that there was a relationship between Issa Doreh and Aden Ayrow or al-Shabaab or that Doreh knew who Ayrow was. Even more significant is the fact that at no time did the government prove, in all of its recorded intercepts that Issa Doreh ever heard the name Sheikalow or Aden Ayrow. Even if Doreh knew Moalin was sending money to Somalia, there was no evidence that he knew this money was being sent to either Ayrow or al-Shabaab or to a terrorist organization or that he did anything other than his job as a clerk at the Shidaal Express – namely to send money from members of the diaspora to Somalia.

In the calls between Issa Doreh and Basaaly Moalin which were introduced at

trial, Moalin never mentioned the name Sheikalow as claimed by the government. Moalin would refer to the "cleric"[66] and there is no evidence that Issa Doreh knew who was "cleric" was or that it was a reference to Ayrow rather than another cleric.

In order to a prove conspiracy, the government must present some evidence from which it can reasonably be inferred that the person charged with conspiracy knew of the existence of the scheme alleged in the indictment and knowingly joined and participated in it." *United States v. Giraldo*, 80 F.3d 667, 673 (2d Cir. 1996).

The parties stipulated and agreed to the following facts: "[I]n early to mid 2008, one, money collected for the Ayr subclan was given to individuals, including Abukar Suryare, AKA Abukar Mohamed, and Farah Shidane, who were associated with the ILEYS charity; two, money colleted by men in Guraceel on behalf of the Ayr subclan was given to a group that was not al-Shabaab; three, there was a (12RT 1732) dispute between al-Shabaab, the Ayr clan, and ILEYS over the administration of the Galgaduud region. Four, members of the ILEYS charity and the Ayr subclan, including Abukar Suryare, were opposed to al-Shabaab and were Ayrow's enemies." (12RT 1732-1733.)

Issa Doreh has been in prison since 2010. The intercepted calls in which he

66 For example, the first call involving Doreh introduced by the government at trial was a call on December 21, 2007 at 07:07:46 (Exhibit 120; 13RT 1867) On that call, Moalin says, "the cleric has just called me" and continued with 'The cleric whom you spoke with the other day."

participated failed to establish that he knew who Sheikalow was, or that he supported al-Shabaab or knew monies were being sent to al-Shabaab, or that he supported terrorism. There is no dispute that monies transferred on July 15, 2008, totaling $2,280 were sent not to al-Shabaab but to Farad Shidane and there is also no dispute that Farah Shidane was not affiliated with al-Shabaab. Government witnesses, as well as Doreh's own words on intercepted calls, proved he was merely a clerk at the Shidaal Express and had no authority over transfers, including no authority over discounts of fees. It must be remembered, according to the government's own expert Bryden, that it was not merely al-Shabaab versus the TFG; it was a broad-based insurgency. In the context of Somali culture, the concept of insurgency refers to a group of regional, clan-based, civil societies that exist autonomously. Government witness Bryden characterized the organizational structure of Somali society as a "segmentary lineage system." (3RT 442-443.)

The government failed to prove that any calls involving Issa Doreh supported a finding that he supported al-Shabaab or terrorism in any way. The calls must be viewed in the context of the slaughter of Somalis by Ethiopians as well as deaths, displacement, and orphans resulting from drought and famine occurring at that time and support by the diaspora of humanitarian relief and the removal of the Ethiopian military from Somali soil.

In assessing sufficiency of the evidence, this Court must determine whether, "after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Jackson v. Virginia*, 443 U.S. at 317. In none of the calls in which Issa Doreh is a participant is there any evidence of his involvement in an agreement to do anything unlawful. There is no agreement as to a conspiracy, to commit murder in Somalia, or to use weapons of mass destruction. There is no evidence at all that Issa Doreh ever knew the name Ayrow, Sheikalow, or al-Shabaab.

In *Jackson v. Virginia,* 443 U.S. at 313-320, the United States Supreme Court held that the Due Process Clause of the 14th Amendment is violated by conviction of a crime without sufficient evidence that each element has been proven beyond a reasonable doubt.[67] It is not enough that Issa Doreh may have known or even associated with the person(s) committing the offenses or unknowingly or unintentionally did things that were helpful to that person or was present at the scene of the crime. The evidence must show beyond a reasonable doubt that he acted with the knowledge and intention of helping that person commit the crimes charged and in that respect, the evidence failed.

---

67 *Bolling v. Sharpe*, 347 U.S. 497 (1954), incorporated the 14th Amendment's guarantee of Due Process from the states to apply to the federal government via the Fifth Amendment's Due Process Clause.

CONCLUSION

These Appellants never supported the al-Shabaab the stance and procedure. This Court should vacate the convictions and remand for a new trial.

Respectfully submitted,

Dated: October 29, 2015

s/Joshua L. Dratel
Joshua Dratel, P.C.
s/Jameel Jaffer
JAMEEL JAFFER
s/Alexander A. Abdo
ALEXANDER A. ABDO
s/Patrick Toomey
PATRICK TOOMEY
s/Brett Max Kaufman
BRETT MAX KAUFMAN
Attorneys for Moalin

S/David J. Zugman
David J. Zugman
Attorney for M. M. Mohamud

S/Elizabeth Armena Missakian
Elizabeth Armena Missakian
Attorney for Issa Doreh

S/Benjamin L. Coleman
Benjamin L. Coleman
Attorney for Ahmed Nasir Taalil Mohamud

CERTIFICATE OF RELATED CASES

Counsel is not aware of any related cases that should be considered with this appeal.

Respectfully submitted,

Dated: October 29, 2015

s/Joshua L. Dratel
Joshua Dratel, P.C.
s/Jameel Jaffer
JAMEEL JAFFER
s/Alexander A. Abdo
ALEXANDER A. ABDO
s/Patrick Toomey
PATRICK TOOMEY
s/Brett Max Kaufman
BRETT MAX KAUFMAN
Attorneys for Moalin

s/David J. Zugman
DAVID J. ZUGMAN
Attorney for M. M. Mohamud

s/Elizabeth Armena Missakian
ELIZABETH ARMENA MISSAKIAN
Attorney for Issa Doreh

s/Benjamin L. Coleman
BENJAMIN L. COLEMAN
Attorney for Ahmed Nasir Taalil Mohamud

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7) and Ninth Circuit Rule 32-1, the attached Opening/~~Answering/Reply~~ Brief is:

Proportionately spaced, has a typeface of 14 points or more, and contains 51725 words.

Dated: October 29, 2015

s/*David J. Zugman*
DAVID J. ZUGMAN

CERTIFICATE OF SERVICE

I hereby certify that on October 29, 2015, I electronically filed the foregoing Appellants' Joint Opening Brief and attached Excerpts of Record with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: October 29, 2015

s/David J. Zugman
DAVID J. ZUGMAN

APPENDIX OF STATUTES

50 U.S.C. §1801. Definitions [Caution: See prospective amendment note below.]

As used in this title [50 USCS §§ 1801 et seq.]:

(a) "Foreign power" means--

(1) a foreign government or any component thereof whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

(b) "Agent of a foreign power" means--

(1) any person other than a United States person, who--

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4), irrespective of whether the person is inside the United States;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of indicate that such person may engage in such activities, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore;

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power, or knowingly aids or abets any person in the conduct of such proliferation or activities in preparation therefor, or knowingly conspires with any person to engage in such

proliferation or activities in preparation therefor; or

(2) any person who--

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

(c) "International terrorism" means activities that--

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended--

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(d) "Sabotage" means activities that involve a violation of chapter 105 of title 18, United States Code [18 USCS §§ 2151 et seq.], or that would involve such a violation if committed against the United States.

(e) "Foreign intelligence information" means--

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

(f) "Electronic surveillance" means--

(1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

(2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code;

(3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

(g) "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General designated as the Assistant Attorney General for National Security under section 507A of title 28, United States Code.

(h) "Minimization procedures", with respect to electronic surveillance, means--

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a) [50 USCS § 1802(a)], procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 [50 USCS § 1805] is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(i) "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act [8 USCS § 1101(a)(20)]), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3).

(j) "United States", when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands.

(k) "Aggrieved person" means a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.

(l) "Wire communication" means any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged

as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.

(m) "Person" means any individual, including any officer or employee of the Federal Government, or any group, entity, association, corporation, or foreign power.

(n) "Contents", when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

(o) "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Trust Territory of the Pacific Islands, and any territory or possession of the United States.

(p) "Weapon of mass destruction" means--

(1) any explosive, incendiary, or poison gas device that is designed, intended, or has the capability to cause a mass casualty incident;

(2) any weapon that is designed, intended, or has the capability to cause death or serious bodily injury to a significant number of persons through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors;

(3) any weapon involving a biological agent, toxin, or vector (as such terms are defined in section 178 of title 18, United States Code) that is designed, intended, or has the capability to cause death, illness, or serious bodily injury to a significant number of persons; or

(4) any weapon that is designed, intended, or has the capability to release radiation or radioactivity causing death, illness, or serious bodily injury to a significant number of persons.

50 U.S.C. §1806. Use of information

(a) Compliance with minimization procedures; privileged communications; lawful purposes. Information acquired from an electronic surveillance conducted pursuant to this title [50 USCS §§ 1801 et seq.] concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title [50 USCS §§ 1801 et seq.]. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this title [50 USCS §§ 1801 et seq.] shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this title [50 USCS §§ 1801 et seq.] may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure. No information acquired pursuant to this title [50 USCS §§ 1801 et seq.] shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States. Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title [50 USCS §§ 1801 et seq.], the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions. Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this title [50 USCS §§ 1801 et seq.], the State or political subdivision thereof shall notify the aggrieved

person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress. Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court. Whenever a court or other authority is notified pursuant to subsection (c) or (d), or whenever a motion is made pursuant to subsection (e), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States of any State before any court or other authority of the United States or any state to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the

surveillance.

(g) Suppression of evidence; denial of motion. If the United States district court pursuant to subsection (f) determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders. Orders granting motions or requests under subsection (g), decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information. In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination. If an emergency employment of electronic surveillance is authorized under subsection (e) or (f) of section 105 [50 USCS § 1805] and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters.

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title [50 USCS §§ 1801 et seq.] may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105 [50 USCS § 1805].

50 U.S.C. § 1825. Use of information

(a) Compliance with minimization procedures; lawful purposes. Information acquired from a physical search conducted pursuant to this title [50 USCS §§ 1821 et seq.] concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this title [50 USCS §§ 1821 et seq.]. No information acquired from a physical search pursuant to this title [50 USCS §§ 1821 et seq.] may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Notice of search and identification of property seized, altered, or reproduced. Where a physical search authorized and conducted pursuant to section 304 [50 USCS § 1824] involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this Act and shall identify any property of such person seized, altered, or reproduced during such search.

(c) Statement for disclosure. No information acquired pursuant to this title [50 USCS §§ 1821 et seq.] shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(d) Notification by United States. Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search pursuant to the authority of this title [50 USCS §§ 1821 et seq.], the United States shall, prior to the trial, hearing, or the other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(e) Notification by States or political subdivisions. Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof against an aggrieved person any information obtained or derived from a physical search pursuant to the authority of this title [50 USCS §§ 1821 et seq.], the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(f) Motion to suppress.

(1) Any person against whom evidence obtained or derived from a physical search to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such search on the grounds that--

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

(2) Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(g) In camera and ex parte review by district court. Whenever a court or other authority is notified pursuant to subsection (d) or (e), or whenever a motion is made pursuant to subsection (f), or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this title [50 USCS §§ 1821 et seq.] or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this title [50 USCS §§ 1821 et seq.], the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the

application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

(h) Suppression of evidence; denial of motion. If the United States district court pursuant to subsection (g) determines that the physical search was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Finality of orders. Orders granting motions or requests under subsection (h), decisions under this section that a physical search was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(j) Notification of emergency execution of physical search; contents; postponement, suspension, or elimination.

(1) If an emergency execution of a physical search is authorized under section 304(d) and a subsequent order approving the search is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of--

(A) the fact of the application;

(B) the period of the search; and

(C) the fact that during the period information was or was not obtained.

(2) On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed

90 days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters.

(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this title [50 USCS §§ 1821 et seq.] may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 303(a)(6) [50 USCS § 1823(a)(6)] or the entry of an order under section 304 [50 USCS § 1824].

50 U.S.C. §1842. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations

(a) Application for authorization or approval.

(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333 [50 USCS § 3001 note], or a successor order.

(2) The authority under paragraph (1) is in addition to the authority under title I of this Act [50 USCS §§ 1801 et seq.] to conduct the electronic surveillance referred to in that paragraph.

(b) Form of application; recipient. Each application under this section shall be in writing under oath or affirmation to--

(1) a judge of the court established by section 103(a) of this Act [50 USCS § 103(a)]; or

(2) a United States Magistrate Judge under chapter 43 of title 28, United States Code [28 USCS §§ 631 et seq.], who is publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders approving the installation and use of a pen register or trap and trace device on behalf of a judge of that court.

(c) Executive approval; contents of application. Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include--

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application;

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is

not conducted solely upon the basis of activities protected by the first amendment to the Constitution; and

(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device.

(d) Ex parte judicial order of approval.

(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section.

(2) An order issued under this section--

(A) shall specify--

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

(B) shall direct that--

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person--

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 105(b)(2)(C) of this Act, any records concerning the pen register or trap and trace device or the aid furnished; and

(iii) the applicant shall compensate such provider, landlord, custodian, or other

person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order--

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order)--

(I) the name of the customer or subscriber;

(II) the address of the customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;

(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;

(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;

(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and

(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order--

(I) the name of such customer or subscriber;

(II) the address of such customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and

(IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

(e) Time limitation.

(1) Except as provided in paragraph (2), an order issued under this section shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days. Extensions of such an order may be granted, but only upon an application for an order under this section and upon the judicial finding required by subsection (d). The period of extension shall be for a period not to exceed 90 days.

(2) In the case of an application under subsection (c) where the applicant has

certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, under this section may be for a period not to exceed one year.

(f) Cause of action barred. No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) in accordance with the terms of an order issued under this section.

(g) Furnishing of results. Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(h) Privacy procedures.

(1) In general. The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

(2) Rule of construction. Nothing in this subsection limits the authority of the court established under section 103(a) [50 USCS § 1803(a)] or of the Attorney General to impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device.

50 U.S.C. §1861. Access to certain business records for foreign intelligence and international terrorism investigations [Caution: See prospective amendment note below.]

(a) Application for order; conduct of investigation generally.

(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall--

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 [50 USCS § 3001 note] (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Recipient and contents of application. Each application under this section--

(1) shall be made to--

(A) a judge of the court established by section 103(a) [50 USCS § 1803(a)]; or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code [28 USCS §§ 631 et seq.], who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall include--

(A) a statement of facts showing that there are reasonable grounds to believe that

the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to--

(i) a foreign power or an agent of a foreign power;

(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c) Ex parte judicial order of approval.

(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) and that the minimization procedures submitted in accordance with subsection (b)(2)(D) meet the definition of minimization procedures under subsection (g), the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) be followed.

(2) An order under this subsection--

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d);

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; and

(E) shall not disclose that such order is issued for purposes of an investigation

described in subsection (a).

(d) Nondisclosure.

(1) No person shall disclose to any other person that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section, other than to--

(A) those persons to whom disclosure is necessary to comply with such order;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2) (A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) (1) No cause of action shall lie in any court against a person who--

(A) produces tangible things or provides information, facilities, or technical assistance in accordance with an order issued or an emergency production required under this section; or

(B) otherwise provides technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of 2015.

(2) A production or provision of information, facilities, or technical assistance described in paragraph (1) shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f) Judicial review of FISA orders.

(1) In this subsection--

(A) the term "production order" means an order to produce any tangible thing under this section; and

(B) the term "nondisclosure order" means an order imposed under subsection (d).

(2) (A) (i) A person receiving a production order may challenge the legality of the production order or any nondisclosure order imposed in connection with the production order that order by filing a petition with the pool established by section 103(e)(1) [50 USCS § 1803(e)(1)]. Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 103(e)(1) [50 USCS § 1803(e)(1)].

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 103(e)(1) [50 USCS § 1803(e)(1)]. Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall promptly consider the petition in accordance with the procedures established under section 103(e)(2) [50 USCS § 1803(e)(2)].

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C) (i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

(ii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing

another such petition with respect to such nondisclosure order.

(iii) [Redesignated]

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 103(b) [50 USCS § 1803(b)], which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) Minimization procedures.

(1) In general. The Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this title [50 USCS §§ 1861 et seq.].

(2) Defined. In this section, the term "minimization procedures" means--

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 101(e)(1) [50 USCS § 1801(e)(1)], shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to

understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(3) Rule of construction. Nothing in this subsection shall limit the authority of the court established under section 103(a) [50 USCS § 1803(a)] to impose additional, particularized minimization procedures with regard to the production, retention, or dissemination of nonpublicly available information concerning unconsenting United States persons, including additional, particularized procedures related to the destruction of information within a reasonable time period.

(h) Use of information. Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title [50 USCS §§ 1861 et seq.] concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g). No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this title [50 USCS §§ 1861 et seq.] shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this title [50 USCS §§ 1861 et seq.] may be used or disclosed by Federal officers or employees except for lawful purposes.

(i) Emergency authority for production of tangible things [Caution: This subsection take effect 180 days after the date of enactment, as provided by § 109(a) of Act June 2, 2015, P.L. 114-23, which appears as a note to this section.].

(1) Notwithstanding any other provision of this section, the Attorney General may require the emergency production of tangible things if the Attorney General--

(A) reasonably determines that an emergency situation requires the production of tangible things before an order authorizing such production can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this section to approve such production of tangible things exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under this section at the time the Attorney General requires the emergency production of tangible things that the decision has been made to employ the authority under this

subsection; and

(D) makes an application in accordance with this section to a judge having jurisdiction under this section as soon as practicable, but not later than 7 days after the Attorney General requires the emergency production of tangible things under this subsection.

(2) If the Attorney General requires the emergency production of tangible things under paragraph (1), the Attorney General shall require that the minimization procedures required by this section for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving the production of tangible things under this subsection, the production shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time the Attorney General begins requiring the emergency production of such tangible things, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 103 [50 USCS 1803].

(5) If such application for approval is denied, or in any other case where the production of tangible things is terminated and no order is issued approving the production, no information obtained or evidence derived from such production shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof, and no information concerning any United States person acquired from such production shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(j) Compensation. The Government shall compensate a person for reasonable expenses incurred for--

(1) producing tangible things or providing information, facilities, or assistance in accordance with an order issued with respect to an application described in subsection (b)(2)(C) or an emergency production under subsection (i) that, to comply with subsection (i)(1)(D), requires an application described in subsection (b)(2)(C); or

(2) otherwise providing technical assistance to the Government under this section or to implement the amendments made to this section by the USA FREEDOM Act of

2015.

(k) Definitions. In this section:

(1) In general. The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" have the meanings provided those terms in section 101 [50 USCS § 1801].

(2) Address. The term "address" means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

(3) Call detail record. The term "call detail record"--

(A) means session-identifying information (including an originating or terminating telephone number, an International Mobile Subscriber Identity number, or an International Mobile Station Equipment Identity number), a telephone calling card number, or the time or duration of a call; and

(B) does not include--

(i) the contents (as defined in section 2510(8) of title 18, United States Code) of any communication;

(ii) the name, address, or financial information of a subscriber or customer; or

(iii) cell site location or global positioning system information.

(4) Specific selection term.

(A) Tangible things.

(i) In general. Except as provided in subparagraph (B), a "specific selection term"--

(I) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

(II) is used to limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things.

(ii) Limitation. A specific selection term under clause (i) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of tangible things sought consistent with the purpose for seeking the tangible things, such as an identifier that--

(I) identifies an electronic communication service provider (as that term is defined in section 701 [50 USCS § 1881]) or a provider of remote computing service (as that term is defined in section 2711 of title 18, United States Code), when not used as part of a specific identifier as described in clause (i), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used

as the basis for the production; or

(II) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in clause (i).

(iii) Rule of construction. Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of clause (i).

(B) Call Detail Record Applications. For purposes of an application submitted under subsection (b)(2)(C), the term "specific selection term" means a term that specifically identifies an individual, account, or personal device.

50 U.S.C. §1881a. Procedures for targeting certain persons outside the United States other than United States persons [Caution: See prospective amendment note below.]

(a) Authorization. Notwithstanding any other provision of law, upon the issuance of an order in accordance with subsection (i)(3) or a determination under subsection (c)(2), the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.

(b) Limitations. An acquisition authorized under subsection (a)--

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

(c) Conduct of acquisition.

(1) In general. An acquisition authorized under subsection (a) shall be conducted only in accordance with--

(A) the targeting and minimization procedures adopted in accordance with subsections (d) and (e); and

(B) upon submission of a certification in accordance with subsection (g), such certification.

(2) Determination. A determination under this paragraph and for purposes of subsection (a) is a determination by the Attorney General and the Director of National Intelligence that exigent circumstances exist because, without immediate implementation of an authorization under subsection (a), intelligence important to the national security of the United States may be lost or not timely acquired and time does not permit the issuance of an order pursuant to subsection (i)(3) prior to the

implementation of such authorization.

(3) Timing of determination. The Attorney General and the Director of National Intelligence may make the determination under paragraph (2)--

(A) before the submission of a certification in accordance with subsection (g); or

(B) by amending a certification pursuant to subsection (i)(1)(C) at any time during which judicial review under subsection (i) of such certification is pending.

(4) Construction. Nothing in title I [50 USCS §§ 1801 et seq.] shall be construed to require an application for a court order under such title for an acquisition that is targeted in accordance with this section at a person reasonably believed to be located outside the United States.

(d) Targeting procedures.

(1) Requirement to adopt. The Attorney General, in consultation with the Director of National Intelligence, shall adopt targeting procedures that are reasonably designed to--

(A) ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(2) Judicial review. The procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(e) Minimization procedures.

(1) Requirement to adopt. The Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 101(h) or 301(4) [50 USCS § 1801(h) or 1821(4)], as appropriate, for acquisitions authorized under subsection (a).

(2) Judicial review. The minimization procedures adopted in accordance with paragraph (1) shall be subject to judicial review pursuant to subsection (i).

(f) Guidelines for compliance with limitations.

(1) Requirement to adopt. The Attorney General, in consultation with the Director of National Intelligence, shall adopt guidelines to ensure--

(A) compliance with the limitations in subsection (b); and

(B) that an application for a court order is filed as required by this Act.

(2) Submission of guidelines. The Attorney General shall provide the guidelines

adopted in accordance with paragraph (1) to--

(A) the congressional intelligence committees;

(B) the Committees on the Judiciary of the Senate and the House of Representatives; and

(C) the Foreign Intelligence Surveillance Court.

(g) Certification.

(1) In general.

(A) Requirement. Subject to subparagraph (B), prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall provide to the Foreign Intelligence Surveillance Court a written certification and any supporting affidavit, under oath and under seal, in accordance with this subsection.

(B) Exception. If the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2) and time does not permit the submission of a certification under this subsection prior to the implementation of an authorization under subsection (a), the Attorney General and the Director of National Intelligence shall submit to the Court a certification for such authorization as soon as practicable but in no event later than 7 days after such determination is made.

(2) Requirements. A certification made under this subsection shall--

(A) attest that--

(i) there are procedures in place that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court that are reasonably designed to--

(I) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;

(ii) the minimization procedures to be used with respect to such acquisition--

(I) meet the definition of minimization procedures under section 101(h) or 301(4) [50 USCS § 1801(h) or 1821(4)], as appropriate; and

(II) have been approved, have been submitted for approval, or will be submitted with the certification for approval by the Foreign Intelligence Surveillance Court;

(iii) guidelines have been adopted in accordance with subsection (f) to ensure compliance with the limitations in subsection (b) and to ensure that an application for

a court order is filed as required by this Act;

(iv) the procedures and guidelines referred to in clauses (i), (ii), and (iii) are consistent with the requirements of the fourth amendment to the Constitution of the United States;

(v) a significant purpose of the acquisition is to obtain foreign intelligence information;

(vi) the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider; and

(vii) the acquisition complies with the limitations in subsection (b);

(B) include the procedures adopted in accordance with subsections (d) and (e);

(C) be supported, as appropriate, by the affidavit of any appropriate official in the area of national security who is--

(i) appointed by the President, by and with the advice and consent of the Senate; or

(ii) the head of an element of the intelligence community;

(D) include--

(i) an effective date for the authorization that is at least 30 days after the submission of the written certification to the court; or

(ii) if the acquisition has begun or the effective date is less than 30 days after the submission of the written certification to the court, the date the acquisition began or the effective date for the acquisition; and

(E) if the Attorney General and the Director of National Intelligence make a determination under subsection (c)(2), include a statement that such determination has been made.

(3) Change in effective date. The Attorney General and the Director of National Intelligence may advance or delay the effective date referred to in paragraph (2)(D) by submitting an amended certification in accordance with subsection (i)(1)(C) to the Foreign Intelligence Surveillance Court for review pursuant to subsection (i).

(4) Limitation. A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted.

(5) Maintenance of certification. The Attorney General or a designee of the Attorney General shall maintain a copy of a certification made under this subsection.

(6) Review. A certification submitted in accordance with this subsection shall be subject to judicial review pursuant to subsection (i).

(h) Directives and judicial review of directives.

(1) Authority. With respect to an acquisition authorized under subsection (a), the Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to--

(A) immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition; and

(B) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such electronic communication service provider wishes to maintain.

(2) Compensation. The Government shall compensate, at the prevailing rate, an electronic communication service provider for providing information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(3) Release from liability. No cause of action shall lie in any court against any electronic communication service provider for providing any information, facilities, or assistance in accordance with a directive issued pursuant to paragraph (1).

(4) Challenging of directives.

(A) Authority to challenge. An electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition to modify or set aside such directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment. The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) [50 USCS § 1803(e)(1)] not later than 24 hours after the filing of such petition.

(C) Standards for review. A judge considering a petition filed under subparagraph (A) may grant such petition only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful.

(D) Procedures for initial review. A judge shall conduct an initial review of a petition filed under subparagraph (A) not later than 5 days after being assigned such petition. If the judge determines that such petition does not consist of claims, defenses, or other legal contentions that are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of such petition and order the recipient to comply with the directive or any part of it. Upon making a determination

under this subparagraph or promptly thereafter, the judge shall provide a written statement for the record of the reasons for such determination.

(E) Procedures for plenary review. If a judge determines that a petition filed under subparagraph (A) requires plenary review, the judge shall affirm, modify, or set aside the directive that is the subject of such petition not later than 30 days after being assigned such petition. If the judge does not set aside the directive, the judge shall immediately affirm or affirm with modifications the directive, and order the recipient to comply with the directive in its entirety or as modified. The judge shall provide a written statement for the record of the reasons for a determination under this subparagraph.

(F) Continued effect. Any directive not explicitly modified or set aside under this paragraph shall remain in full effect.

(G) Contempt of court. Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(5) Enforcement of directives.

(A) Order to compel. If an electronic communication service provider fails to comply with a directive issued pursuant to paragraph (1), the Attorney General may file a petition for an order to compel the electronic communication service provider to comply with the directive with the Foreign Intelligence Surveillance Court, which shall have jurisdiction to review such petition.

(B) Assignment. The presiding judge of the Court shall assign a petition filed under subparagraph (A) to 1 of the judges serving in the pool established under section 103(e)(1) [50 USCS § 1803(e)(1)] not later than 24 hours after the filing of such petition.

(C) Procedures for review. A judge considering a petition filed under subparagraph (A) shall, not later than 30 days after being assigned such petition, issue an order requiring the electronic communication service provider to comply with the directive or any part of it, as issued or as modified, if the judge finds that the directive meets the requirements of this section and is otherwise lawful. The judge shall provide a written statement for the record of the reasons for a determination under this paragraph.

(D) Contempt of court. Failure to obey an order issued under this paragraph may be punished by the Court as contempt of court.

(E) Process. Any process under this paragraph may be served in any judicial district in which the electronic communication service provider may be found.

(6) Appeal.

(A) Appeal to the Court of Review. The Government or an electronic

communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition with the Foreign Intelligence Surveillance Court of Review for review of a decision issued pursuant to paragraph (4) or (5). The Court of Review shall have jurisdiction to consider such petition and shall provide a written statement for the record of the reasons for a decision under this subparagraph.

(B) Certiorari to the Supreme Court. The Government or an electronic communication service provider receiving a directive issued pursuant to paragraph (1) may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(i) Judicial review of certifications and procedures.

(1) In general.

(A) Review by the Foreign Intelligence Surveillance Court. The Foreign Intelligence Surveillance Court shall have jurisdiction to review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e), and amendments to such certification or such procedures.

(B) Time period for review. The Court shall review a certification submitted in accordance with subsection (g) and the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and shall complete such review and issue an order under paragraph (3) not later than 30 days after the date on which such certification and such procedures are submitted.

(C) Amendments. The Attorney General and the Director of National Intelligence may amend a certification submitted in accordance with subsection (g) or the targeting and minimization procedures adopted in accordance with subsections (d) and (e) as necessary at any time, including if the Court is conducting or has completed review of such certification or such procedures, and shall submit the amended certification or amended procedures to the Court not later than 7 days after amending such certification or such procedures. The Court shall review any amendment under this subparagraph under the procedures set forth in this subsection. The Attorney General and the Director of National Intelligence may authorize the use of an amended certification or amended procedures pending the Court's review of such amended certification or amended procedures.

(2) Review. The Court shall review the following:

(A) Certification. A certification submitted in accordance with subsection (g) to

determine whether the certification contains all the required elements.

(B) Targeting procedures. The targeting procedures adopted in accordance with subsection (d) to assess whether the procedures are reasonably designed to--

(i) ensure that an acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and

(ii) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

(C) Minimization procedures. The minimization procedures adopted in accordance with subsection (e) to assess whether such procedures meet the definition of minimization procedures under section 101(h) [50 USCS § 1801(h)] or section 301(4) [50 USCS § 1821(4)], as appropriate.

(3) Orders.

(A) Approval. If the Court finds that a certification submitted in accordance with subsection (g) contains all the required elements and that the targeting and minimization procedures adopted in accordance with subsections (d) and (e) are consistent with the requirements of those subsections and with the fourth amendment to the Constitution of the United States, the Court shall enter an order approving the certification and the use, or continued use in the case of an acquisition authorized pursuant to a determination under subsection (c)(2), of the procedures for the acquisition.

(B) Correction of deficiencies. If the Court finds that a certification submitted in accordance with subsection (g) does not contain all the required elements, or that the procedures adopted in accordance with subsections (d) and (e) are not consistent with the requirements of those subsections or the fourth amendment to the Constitution of the United States, the Court shall issue an order directing the Government to, at the Government's election and to the extent required by the Court's order--

(i) correct any deficiency identified by the Court's order not later than 30 days after the date on which the Court issues the order; or

(ii) cease, or not begin, the implementation of the authorization for which such certification was submitted.

(C) Requirement for written statement. In support of an order under this subsection, the Court shall provide, simultaneously with the order, for the record a written statement of the reasons for the order.

(D) Limitation on use of information.

(i) In general. Except as provided in clause (ii), if the Court orders a correction of a deficiency in a certification or procedures under subparagraph (B), no

information obtained or evidence derived pursuant to the part of the certification or procedures that has been identified by the Court as deficient concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired pursuant to such part of such certification or procedures shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(ii) Exception. If the Government corrects any deficiency identified by the order of the Court under subparagraph (B), the Court may permit the use or disclosure of information obtained before the date of the correction under such minimization procedures as the Court may approve for purposes of this clause.

(4) Appeal.

(A) Appeal to the Court of Review. The Government may file a petition with the Foreign Intelligence Surveillance Court of Review for review of an order under this subsection. The Court of Review shall have jurisdiction to consider such petition. For any decision under this subparagraph affirming, reversing, or modifying an order of the Foreign Intelligence Surveillance Court, the Court of Review shall provide for the record a written statement of the reasons for the decision.

(B) Continuation of acquisition pending rehearing or appeal. Any acquisition affected by an order under paragraph (3)(B) may continue--

(i) during the pendency of any rehearing of the order by the Court en banc; and

(ii) if the Government files a petition for review of an order under this section, until the Court of Review enters an order under subparagraph (C).

(C) Implementation pending appeal. Not later than 60 days after the filing of a petition for review of an order under paragraph (3)(B) directing the correction of a deficiency, the Court of Review shall determine, and enter a corresponding order regarding, whether all or any part of the correction order, as issued or modified, shall be implemented during the pendency of the review.

(D) Certiorari to the Supreme Court. The Government may file a petition for a writ of certiorari for review of a decision of the Court of Review issued under subparagraph (A). The record for such review shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(5) Schedule.

(A) Reauthorization of authorizations in effect. If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a), the Attorney General and the Director of National Intelligence shall, to the extent practicable, submit to the Court the certification prepared in accordance with subsection (g) and the procedures adopted in accordance with subsections (d) and (e) at least 30 days prior to the expiration of such authorization.

(B) Reauthorization of orders, authorizations, and directives. If the Attorney General and the Director of National Intelligence seek to reauthorize or replace an authorization issued under subsection (a) by filing a certification pursuant to subparagraph (A), that authorization, and any directives issued thereunder and any order related thereto, shall remain in effect, notwithstanding the expiration provided for in subsection (a), until the Court issues an order with respect to such certification under paragraph (3) at which time the provisions of that paragraph and paragraph (4) shall apply with respect to such certification.

(j) Judicial proceedings.

(1) Expedited judicial proceedings. Judicial proceedings under this section shall be conducted as expeditiously as possible.

(2) Time limits. A time limit for a judicial decision in this section shall apply unless the Court, the Court of Review, or any judge of either the Court or the Court of Review, by order for reasons stated, extends that time as necessary for good cause in a manner consistent with national security.

(k) Maintenance and security of records and proceedings.

(1) Standards. The Foreign Intelligence Surveillance Court shall maintain a record of a proceeding under this section, including petitions, appeals, orders, and statements of reasons for a decision, under security measures adopted by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(2) Filing and review. All petitions under this section shall be filed under seal. In any proceedings under this section, the Court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions of a submission, which may include classified information.

(3) Retention of records. The Attorney General and the Director of National Intelligence shall retain a directive or an order issued under this section for a period

of not less than 10 years from the date on which such directive or such order is issued.

(l) Assessments and reviews.

(1) Semiannual assessment. Not less frequently than once every 6 months, the Attorney General and Director of National Intelligence shall assess compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f) and shall submit each assessment to--

(A) the Foreign Intelligence Surveillance Court; and

(B) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution--

(i) the congressional intelligence committees; and

(ii) the Committees on the Judiciary of the House of Representatives and the Senate.

(2) Agency assessment. The Inspector General of the Department of Justice and the Inspector General of each element of the intelligence community authorized to acquire foreign intelligence information under subsection (a), with respect to the department or element of such Inspector General--

(A) are authorized to review compliance with the targeting and minimization procedures adopted in accordance with subsections (d) and (e) and the guidelines adopted in accordance with subsection (f);

(B) with respect to acquisitions authorized under subsection (a), shall review the number of disseminated intelligence reports containing a reference to a United States-person identity and the number of United States-person identities subsequently disseminated by the element concerned in response to requests for identities that were not referred to by name or title in the original reporting;

(C) with respect to acquisitions authorized under subsection (a), shall review the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(D) shall provide each such review to--

(i) the Attorney General;

(ii) the Director of National Intelligence; and

(iii) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution--

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the Senate.

(3) Annual review.

(A) Requirement to conduct. The head of each element of the intelligence community conducting an acquisition authorized under subsection (a) shall conduct an annual review to determine whether there is reason to believe that foreign intelligence information has been or will be obtained from the acquisition. The annual review shall provide, with respect to acquisitions authorized under subsection (a)--

(i) an accounting of the number of disseminated intelligence reports containing a reference to a United States-person identity;

(ii) an accounting of the number of United States-person identities subsequently disseminated by that element in response to requests for identities that were not referred to by name or title in the original reporting;

(iii) the number of targets that were later determined to be located in the United States and, to the extent possible, whether communications of such targets were reviewed; and

(iv) a description of any procedures developed by the head of such element of the intelligence community and approved by the Director of National Intelligence to assess, in a manner consistent with national security, operational requirements and the privacy interests of United States persons, the extent to which the acquisitions authorized under subsection (a) acquire the communications of United States persons, and the results of any such assessment.

(B) Use of review. The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall use each such review to evaluate the adequacy of the minimization procedures utilized by such element and, as appropriate, the application of the minimization procedures to a particular acquisition authorized under subsection (a).

(C) Provision of review. The head of each element of the intelligence community that conducts an annual review under subparagraph (A) shall provide such review to--

(i) the Foreign Intelligence Surveillance Court;

(ii) the Attorney General;

(iii) the Director of National Intelligence; and

(iv) consistent with the Rules of the House of Representatives, the Standing Rules of the Senate, and Senate Resolution 400 of the 94th Congress or any successor Senate resolution--

(I) the congressional intelligence committees; and

(II) the Committees on the Judiciary of the House of Representatives and the

Senate.